Patrocinado por

COR Technologies

Consultora en Capacitación Informática
Consultora en Seguridad Informática

WWW.CORTECH.COM.AR

distribución gratuita

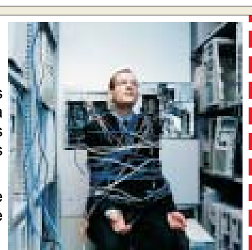


PERIODICO DE NETWORKING

n°9

JUNIO 2004

Wireless: presente y futuro



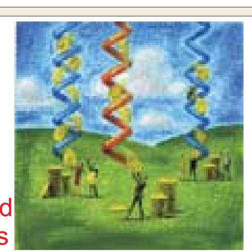
Las posibilidades de las actuales redes inalámbricas y de telefonía celular nos asombran. El wireless del futuro es muchísimo más espectacular.

Conozca las tecnologías que gobiernan al mundo wireless de hoy y las de mañana

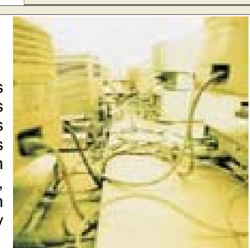
Null sessions o login anónimo.

El ABC de VPNs

VPNs como seguridad en redes inalámbricas



MCSA y MCSE a fondo



Conozca porqué son importantes las certificaciones que nos propone Microsoft para quienes hacen infraestructura de redes (networking). Describimos en detalle cada una de ellas. Además, es posible realizar una orientación (especialización): security y messaging.

Wireless Presente

Wi-Fi Bluetooth RFID

VS.

Wi-Max Zigbee Mobil-Fi Ultrawideband

Wireless Futuro

editorial

En esta edición de NEX (NEX9) analizamos las tecnologías wireless que son utilizadas hoy: WiFi, Bluetooth, RFID y otras.

Todavía quedamos asombrados de lo que es posible hacer hoy con nuestras laptops, PDAs y teléfonos celulares. Pero, ¿cuál es el futuro? Seguramente quedará impactado de lo que se podrá hacer cuando comiencen a ponerse en funcionamiento una serie de nuevas tecnologías. En una serie de artículos analizamos el wireless de hoy y del mañana, su impacto económico y cómo modificará nuestras vidas.

Para poder entender wireless debemos entender los conceptos esenciales de las ondas electromagnéticas. En el artículo “Teoría sobre las ondas electromagnéticas” le damos los conceptos básicos. Para los muchos que se han suscripto a NEX recientemente hemos vuelto a imprimir una serie de excelentes artículos extractados de números anteriores. Temas como: “ABC de VPNs”, “VPN la solución para seguridad en redes inalámbricas usando W2K”,”Entendiendo IPsec” y “Todo sobre null sessions o Login anónimo” son algunos de éstos.

Analizamos en detalle las certificaciones de Microsoft de infraestructura (networking) MCSA y MCSE.

Finalmente, en la página 22 lo empapamos sobre la ISO /IEC 17799 y su relación al estándar Británico BS 7799-1 y 2.



Staff

Año 3 - Número 9 - Junio 2004

Director
Dr. Osvaldo Rodríguez

Propietarios
COR Technologies S.R.L.

Coordinador Editorial
Carlos Rodríguez Bontempi

Coordinación General
María Luján Zito

Responsable de Contenidos
Dr. Osvaldo Rodríguez

Editor en Jefe
Raúl Kuzner

Redactores
Martín Sturm, Javier Pierini, Raúl Kuzner, Osvaldo Rodríguez, María Luján Zito, Leonel F. Becchio, Rodrigo M. González, Hugo Cela, Guido Lorenzutti.

Humor
Marcos Severi

Distribución
Paola Karvouniaris, Ximena Antona

Diseño Web Site
Emanuel A. Rincón

Diseño Gráfico
Víctor Pereyra
Carlos Rodríguez Bontempi

Publicidad
Ximena Antona
publicidad@nexweb.com.ar
+54 (11) 4312-7694

Preimpresión e Impresión
Talleres Gráficos S.A.
Buenos Aires Herald Ltd.Ind.Fin.
Azopardo 455
C1107ADE - Capital Federal

NEX - Periódico de Networking
Registro de la propiedad Intelectual en trámite leg3038

Dirección: Av. Córdoba 657, Piso 12
C1054AAF - Capital Federal
Tel: +54 (11) 4312-7694
http://www.nexweb.com.ar

El staff de NEX colabora ad-honorem, si desea escribir para nosotros, enviar un e-mail a: articulos@nexweb.com.ar

Retire su ejemplar NEX en forma gratuita en Av.Córdoba 657, Piso 12 - Capital Federal o solicítelo telefónicamente para su empresa al +54 (11) 4312-7694
http:// www.nexweb.com.ar



El ABC de las redes inalámbricas y Access Points - Wi Fi

Existen en la actualidad un número grande de productos fácilmente configurables y de bajo precio que nos permiten establecer una red "wireless" (inalámbrica). Esta red puede estar compuesta por un conjunto de máquinas cada una con una NIC (Network Interface Card - Tarjeta de red) inalámbrica que se comunican entre sí en una configuración llamada "peer to peer" o modo ad-hoc. O, la arquitectura mas frecuente hoy día (y la que describimos aquí): la tecnología de Access Point (AP).

La flexibilidad, conveniencia y ahorro tientan a las compañías a hacer conexiones inalámbricas entre edificios o través de un campus. Estas wireless LAN (WLAN) están basadas en su mayoría en la tecnología 802.11b.
Veremos someramente las nuevas tecnologías WLAN y como funcionan. Básicamente, la tecnología AP y el concepto de roaming y asociación.
La típica infraestructura WLAN (ver Figura 1) consiste en múltiples APs conectados cada uno por cable a una LAN para formar un puente transparente para clientes inalámbricos. Los clientes inalámbricos son por ejemplo, computadoras portátiles, desktops o PDAs que tienen tarjetas inalámbricas de acceso compatibles y utilizan un protocolo de radio a una dada frecuencia para comunicarse. Los APs generalmente proporcionan una manera transparente de conectar un dispositivo inalámbrico a una red cableada. Cuando un cliente inalámbrico se conecta y autentica (se asocia) a un AP, el cliente puede solicitar una dirección IP y acceder a los recursos de la red.

La Tecnología

La tecnología DSSS (Direct Sequence Spread Spectrum) desarrollada por las Fuerzas Armadas de USA es particularmente resistente a interferencia e interrupción. La mayoría de los AP 802.11b usa esta tecnología. Opera básicamente a 2.4 Ghz en la banda de frecuencia llamada ISM (Industrial Scientific and Medical)
Esta soporta canales desde 11 Mhz a 22 Mhz (3 de ellos de 1,6 y 11 no se sobreponen). La tecnología 802.11b realiza la transferencia de datos en forma half duplex de 1Mbps, 2 Mbps, 5.5 Mbps y 11 Mbps.
Existe otra alternativa, la 802.11a que usa *OFDM (Orthogonal Frequency Division Multiplexing) que opera en la banda de frecuencia de 5 Ghz y soporta hasta 54 Mbps y 8 canales que no se superponen.*
802.11b es mas lenta que 802.11a pero es mas popular y sus costos mucho menores. Recordar que estos estándares NO son compatibles (Ver el recuadro sobre la nueva tecnología 802.11g).

Figura 1

Wired Server
Wired Client
Ethernet Lan
AP2
Wireless Client
Wireless Client
AP1
Wireless Client

Las figuras 1, 2 y 3 nos muestran las mas típicas arquitecturas wireless basadas en tecnología AP.
En el caso de la Fig. 1 cada AP nos conecta directamente a la LAN. Esto normalmente con cable categoría 5. Tener múltiples AP nos extiende la WLAN y permite a usuarios móviles hacer "roaming" (deambular) en nuestras oficinas o campus.
La segunda posibilidad nos la ilustra la figura 2. Algunos APs pueden actuar como "puente inalámbrico" (wireless bridge) entre por ejemplo, dos edificios cercanos. Aquí la tecnología de antenas se vuelve mas sofisticada (por ejemplo, aparecen antenas unidireccionales) de modo de extender las distancias y aprovechar las altas ganancias de recepción y emisión (Ver www.cortech.com.ar A veces un AP se conecta a otro AP lo que permite extender el rango de área cubierta. Un AP opera como repetidor. La Fig. 3 muestra esta tercera arquitectura. Debido que el AP debe recibir y retransmitir datos, la salida se ve reducida en un factor 2 por cada repetidor de la cadena.
Como curiosidad comentamos que la IETF (Internet Engineering Task Force) trabaja en un "mobile IP Standard" (RFC 3344 ftp://ftp.isi.edu.in-notes/rfc3344.txt). "Mobile IP" es una modificación de TCP/IP que asigna al cliente wireless dos direcciones IP: una "home" y otra "care-of". El sistema operativo y aplicaciones se ligan a la "home" y este IP no se modifica. La IP "care-of" se asocia con la subred del AP al cual este cliente se asocia. Y, puede cambiar dinámicamente dependiendo del AP que se conecte.
Finalmente, describamos los conceptos de "Roaming" y Asociación. Cuando uno inicia un cliente wireless, éste localiza y se "asocia" al mejor AP. Utilizando un protocolo de radio, distingue cual es el "mejor" AP. "Mejor" típicamente incluye calidad de la señal y carga en el AP (pero no necesariamente cercanía).
Cuando el cliente hace *"roaming"* la calidad de señal entre el cliente y el AP se deteriora, lo que causa que el cliente se disocie. Roaming es la característica que le permite al cliente moverse de AP en AP sin dejar caer su conexión de red. Quizás uno participe de una conferencia en la biblioteca de la empresa y luego con su laptop se dirija a su oficina. En este momento la calidad de la señal es posible que se degrade y el cliente wireless se asocia a otro AP.

802.11g Nueva Tecnología

Ya están a la venta productos wireless (inalámbricos) que funcionarán bajo la norma *IEEE 802.11g.* Este protocolo permite a la red comunicarse a 54 Mbps, un factor 5 respecto del más común usado hoy el *802.11b* de 11 Mbps. Lo muy interesante es que *"g" es* compatible 100% con la tecnología *"b"*.



Figura2

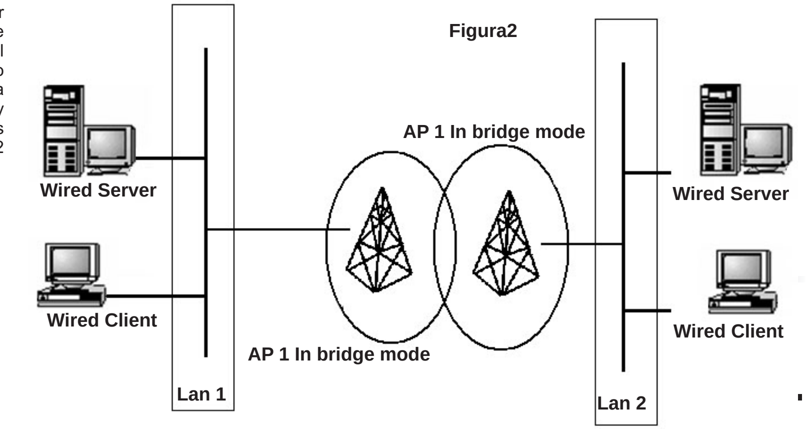
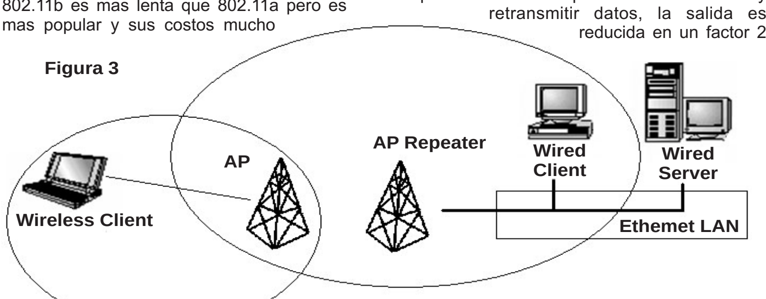


Figura 3



Bluetooth: Tecnología del presente

Estamos inmersos en un mundo tecnológico donde cada vez con mayor frecuencia percibimos términos que en cierta manera nos confunden a la hora de elegir ciertos dispositivos. Bluetooth es uno de ellos, un estándar de las comunicaciones inalámbricas que promete un futuro acelerado.

Si hablamos de comunicaciones, para transmitir información de un sitio a otro, se necesita contar con un canal por el cual viajará la señal que representa tal información. Podemos hacerlo a través de lo que se denominan medios guiados como son los cables (señales eléctricas) o fibras ópticas (señales ópticas), y por medios no guiados como son los enlaces inalámbricos. Por inalámbrico entendemos "sin cables". Es verdad, prescindiremos de cables ya que la transmisión se realiza por ondas electromagnéticas (Ver **Teoría sobre**...Pag 9)

Redes Inalámbricas

Los enlaces por ondas electromagnéticas han posibilitado el surgimiento de las redes inalámbricas. Las **WLAN** o *Wireless Local Area Network* son redes de igual a igual dentro de un edificio, pequeña área residencial o campus universitario que permiten interconectar equipos sin la utilización de cables, en su lugar utiliza ondas electromagnéticas para enviar y recibir datos. Éstas redes operan bajo el estándar IEEE 802.11 y sus variantes, acordadas por el Instituto de Ingenieros Eléctricos y Electrónicos, que definen las especificaciones técnicas con las que deben operar dichas redes. Al conjunto de dichos estándares se los han denominado tecnología Wi-Fi (**W**ireless **Fi**delity, *Fidelidad Inalámbrica*). De este modo existen diferentes estándares que comprenden diferentes tasas de transmisión de datos, áreas de cobertura, etc. Las redes WLAN se componen de dos tipos de elementos, los puntos de acceso y los dispositivos de cliente. Los puntos de acceso actúan como concentradores que reciben o envían información a los dispositivos clientes que generalmente son una PC o PDA (Palm o Pocket PC). Es muy común encontrar notebooks, Palms o Pocket PC que incluyan soporte para Wi-Fi, esto les sirve para integrarse a una red sin cables donde es posible compartir datos entre dispositivos e incluso la conexión a Internet. Para ello se conecta el punto de acceso a la Internet a través de por ejemplo la red telefónica y, cada dispositivo cliente dispondrá de dicha conexión en forma inalámbrica dentro del área de cobertura. Las tasas de transferencia de datos que definen Wi-Fi llegan como máximo a los 54Mbps (según el estándar) velocidad suficiente para una comunicación efectiva entre dispositivos. Un caso particular de este tipo de redes son las **WPAN** o *Wireless Personal Area Network* que limitan su funcionamiento a un área personal de 10 metros. Para su utilización se ha creado un estándar más reducido que Wi-Fi con propósitos similares: **Bluetooth**.

INTERNET
WAN
WI-FI
WI-FI
PERSONAL AREA NETWORK
BLUETOOTH

Figura 1

Bluetooth

Este estándar nace a principios de 1998 impulsado por las firmas Ericsson y Nokia y actualmente apoyado por más de 2000 empresas internacionales que forman lo que se denomina SIG (Special Interest Group) donde cada empresa adopta esta tecnología para fabricar sus productos. La idea surge por la necesidad de interconectar dispositivos personales tales como palmtops, teléfonos celulares, etc para formar una red de área personal o PAN (**P**ersonal **A**rea **N**etwork). Al contar con el apoyo de la industria informática y de telecomunicaciones, en cierta medida se garantiza su éxito.

Explicamos el porqué del nombre. La razón es que en el siglo X el rey Harald II de Dinamarca, apodado "diente azul" (Bluetooth), a causa de una enfermedad que le daba ésta coloración a su dentadura, reunificó bajo su reinado numerosos pequeños reinos que existían en Dinamarca y Noruega y que funcionaban con reglas distintas, lo mismo que hace la tecnología Bluetooth, promovida por Ericsson (Suecia) y Nokia (Finlandia), dos países escandinavos.

Hace años que estos dispositivos se venían comunicando con haces infrarrojos a través de puertos preparados para tal fin, pero dicha comunicación posee la particularidad de ser altamente direccional con lo cual los dispositivos deben ubicarse enfrentados y a muy corta distancia. Esto, a pesar de no necesitar cables, crea la incomodidad de tener que ubicar los dispositivos en forma cercana. Bluetooth soluciona esto gracias a que opera en la banda de 2,4 GHz y su antena emite en forma omnidireccional lo cual permite comunicarse con dispositivos dentro de su radio de alcance en forma no visible.

RED GPRS O UMTS
BLUETOOTH
TELÉFONO CELULAR
PDA

Figura 3

Las redes que operan con tecnología Wi-Fi permiten alcanzar distancias de hasta 100 metros y tasas de transferencia de hasta 54 Mb/s (mega bits por segundo) según sea el estándar. Esto es suficiente para lograr una red de área local inalámbrica (Wireless LAN) sin necesidad de montar cables. El objetivo de Bluetooth, en cambio es lograr la intercomunicación entre dispositivos personales como teléfonos celulares, palmtops, auriculares, etc para lo cual no se necesitan ni tasas de transferencias tan altas ni cubrir distancias tan amplias como en el caso de las redes de área local. Es por eso que decimos que se trata de un estándar reducido pero no por eso poco potente. Esto es básicamente lo que diferencia Bluetooth de Wi-Fi, ambos estándares para redes inalámbricas.

En el marco del

▶▷

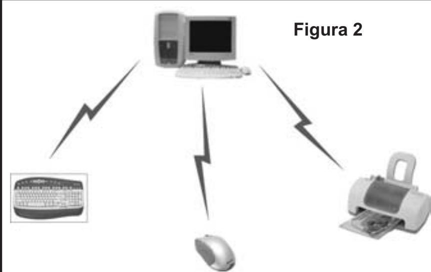


Figura 2

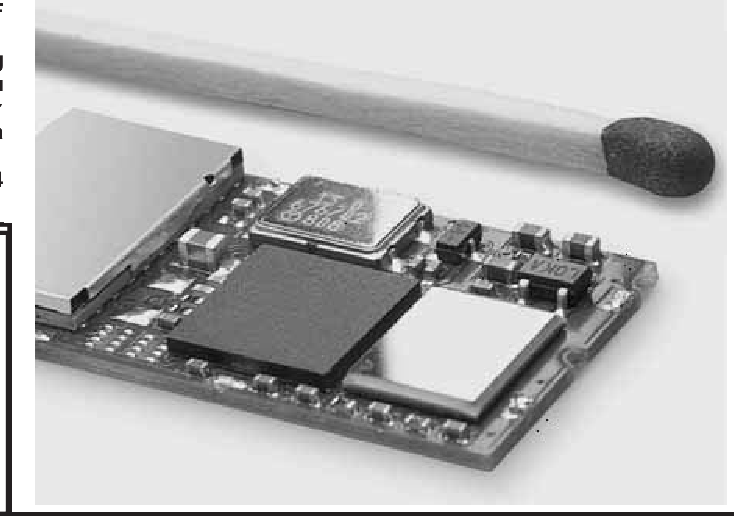


Figura 4

estándar 802.11 para redes LAN, surge Bluetooth (IEEE 802.15) como tecnología de reemplazo de los haces infrarrojos. El estándar define una frecuencia de trabajo de 2,4 GHz (miles de millones de ciclos por segundo). Esta banda de frecuencias no se encuentra licenciada en ningún país por lo que su uso indiscriminado puede traer aparejadas interferencias de diversa índole. Tal es el caso de la banda de operación de los hornos microondas, frecuencia necesaria para lograr la vibración de las moléculas de agua contenida en los alimentos. Para solventar el tema de las interferencias, el estándar no asigna una única frecuencia de trabajo sino que asigna una gama que va de los 2,402 GHz a los 2,480 GHz, esta técnica se conoce como *espectro extendido (spread spectrum). Dentro de esta gama, el transmisor produce saltos de frecuencia aleatorios de a 1 MHz a razón de 1600 saltos por segundo transmitiendo durante 625 μs (micro segundos, millonésimas de segundo) en cada* frecuencia. Esta técnica es conocida como *frequency hopping. Ambas técnicas se conocen como* **FHSS (Frequency Hopping Spread Spectrum).**

Con esto se logran dos cosas, por una parte reducir alguna posible interferencia momentánea en determinada frecuencia y, por otra parte contribuir a mantener la seguridad de la información que se transmite. ¿Cómo es esto? Vamos a suponer que contamos con algunos dispositivos que posean la tecnología Bluetooth, los mismos forman parte de lo que se denomina una piconet o picorred. Uno de estos dispositivos, el que origina la petición de transmisión, se denomina maestro y los demás esclavos. Como es de sospechar, los dispositivos esclavos obedecen las órdenes del maestro. Éste último les comunica a los demás cómo serán las pautas de transmisión, entre ellas cómo se harán los saltos de frecuencia. Una vez pactado esto, se comienza a transmitir. De esta manera, si algún dispositivo no autorizado ingresa a la picorred desde el exterior, al no conocer la secuencia de saltos acordada previamente, no podrá seguir la transmisión en forma completa. Probablemente y con esfuerzo logre captar algunos paquetes enviados pero nunca la transmisión completa. Otras medidas de seguridad incorporadas son la encriptación de los datos con una longitud de clave de hasta 64 bits y la autenticación a nivel de capa de aplicación. Esto demuestra que no es tan fácil comprometer la seguridad de estos dispositivos.

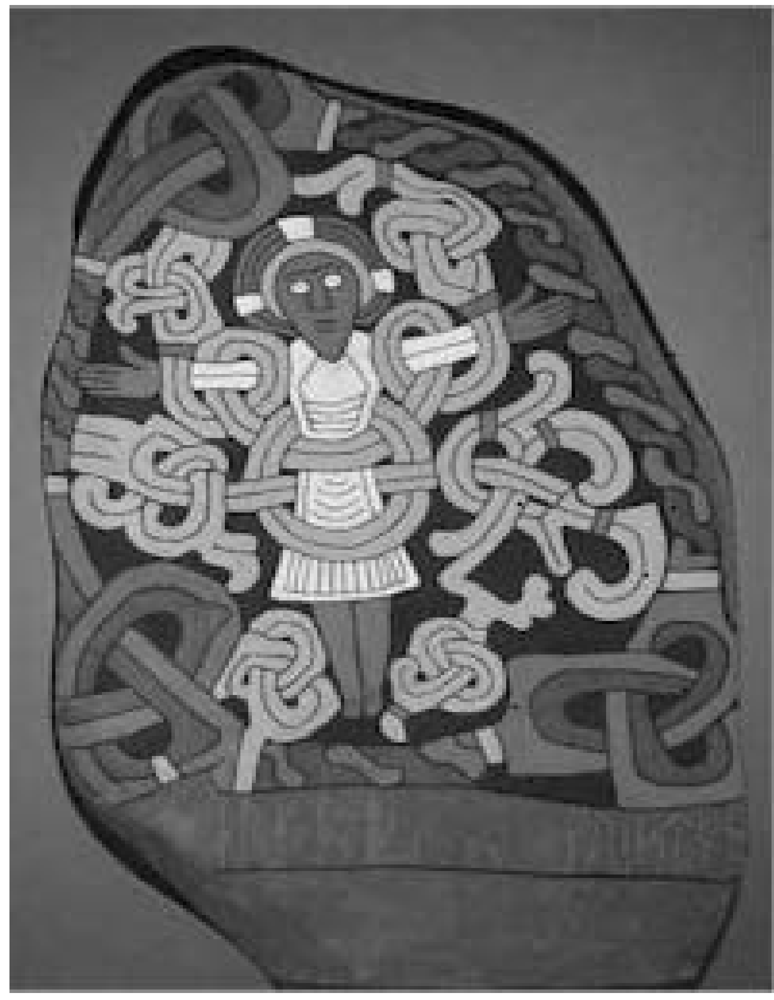


Figura 5 Rey Harald II “Bluetooth”

Bluetooth soporta transmisión de voz y datos. Posee tres canales de voz que admiten transferencias de hasta 64 Kb/s y dos canales de datos. Las transmisiones de datos pueden ser asimétricas, es decir 721 Kb/s en emisión y 57,6 Kb/s en recepción o, si el enlace es simétrico, las tasas de transferencia son de 432,6 Kb/s para cada canal.

Su tasa máxima de transferencia es de 1 Mb/s suficiente para la comunicación entre dispositivos personales y posee un alcance máximo de 10 metros con 1mW de potencia de transmisión. Mediante amplificadores se pueden lograr unos 100 mW para cubrir zonas de hasta 100 metros pero esta implementación trae aparejada una inseparable distorsión en la señal. Se pueden agrupar hasta 7 dispositivos para que formen una picorred y hasta 10 picorredes pueden convivir en la misma zona de cobertura.

Bluetooth se ha diseñado como un sistema de bajo consumo de energía ideal para equipos portátiles, lo que implica bajas potencias de transmisión, suficientes para entornos domésticos. El módulo transmisor receptor (transceiver) de alrededor de media pulgada se alimenta con 2,7 Volts. Para minimizar el consumo de las baterías que lo alimentan, si los dispositivos Bluetooth no intercambian datos, entonces establecen el modo de “espera” para ahorrar energía, quedando a la escucha de mensajes. Ejemplos de aplicación bluetooth son la interconexión de periféricos a una computadora (figura 2) o el acceso a Internet mediante una PDA y un teléfono celular (figura 3). Este último ejemplo nos permitiría obtener Internet móvil dado el uso del teléfono celular.

En memoria del Rey Harald II, la compañía Ericsson, creadora e impulsora de la tecnología Bluetooth, levantó en septiembre de 1999 una nueva piedra en su homenaje delante de su sede en Lund, Suecia.

Leonardo Becchio



Figura 6
Personal de Ericsson inaugurando el monumento a Harald II “Bluetooth” en su sede de Lund, Suecia

Indice Wireless

TEORÍA SOBRE LAS ONDAS ELECTROMAGNÉTICAS

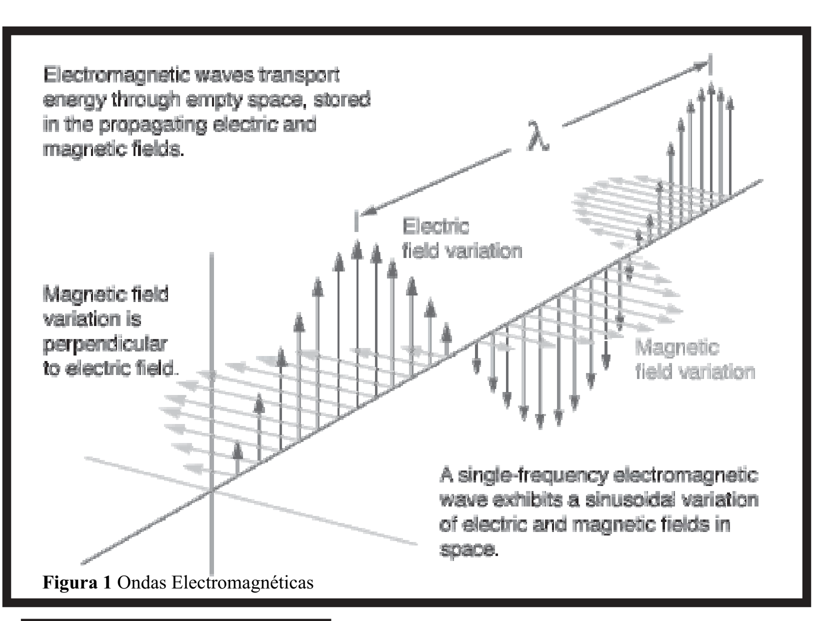


Figura 1 Ondas Electromagnéticas

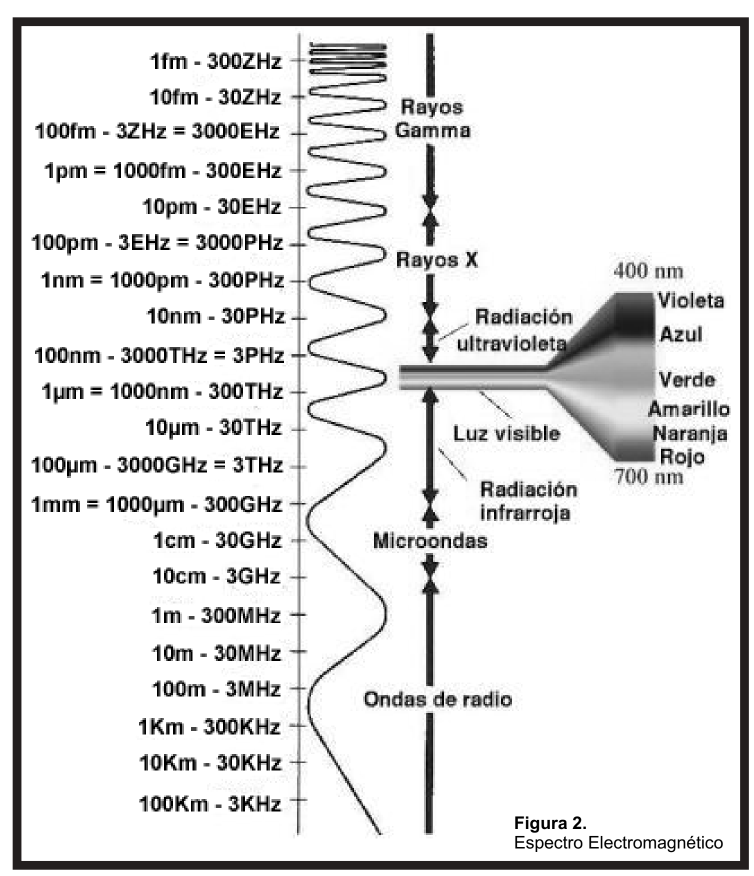


Figura 2.
Espectro Electromagnético

Nota: Generalmente las ondas electromagnéticas superiores a la franja de microondas son denominadas por su longitud de onda en términos de nanometros y no por su frecuencia. A pesar de esto decidimos hacer una comparación cuantitativa. La denominación de cada prefijo podrá encontrarla en la siguiente tabla:

Factor	Nombre	Símbolo
10^{24}	yotta	Y
10^{21}	zetta	Z
10^{18}	exa	E
10^{15}	peta	P
10^{12}	tera	T
10^{9}	giga	G
10^{6}	mega	M
10^{3}	kilo	K o k
10^{2}	hecto	h
10	deca	Da o D
10^{-1}	deci	d
10^{-2}	centi	c
10^{-3}	mili	m
10^{-6}	micro	μ
10^{-9}	nano	n
10^{-12}	pico	p
10^{-15}	femto	f
10^{-18}	atto	a
10^{-21}	zepto	z
10^{-24}	yocto	y

Como su nombre lo indica, las ondas electromagnéticas son campos eléctricos y magnéticos que oscilan en cuadratura (perpendiculares) a una frecuencia dada. Definimos como frecuencia a la cantidad de ciclos por segundos que desarrolla una onda, su unidad son los ciclos por segundo (c/s) o simplemente Hertz (Hz). Según su frecuencia, las ondas sufren una clasificación que permite acomodarlas dentro de un espectro bien definido.Dentro de este espectro se encuentra una franja correspondiente a frecuencias de ondas electromagnéticas pertenecientes a la luz visible, cuyos extremos se encuentran acotados por frecuencias por debajo de la del rojo (infrarrojos) y por frecuencias que se hallan por encima de la del violeta (ultravioleta). Dentro de esa gama se hallan todas las frecuencias correspondientes a las ondas electromagnéticas que dan origen a la luz visible por nuestros ojos.

También vemos una banda comprendida por ondas de muy corta longitud como son las microondas (aprox. 3 GHz a 300 GHz), muy utilizadas para realizar enlaces. Siguiendo hacia abajo encontramos ondas de radio de mayor longitud (menor frecuencia) como las utilizadas para la transmisión de televisión, radio AM-FM, etc. Estas ondas a su vez se clasifican en EHF (Extremada Alta Frecuencia), UHF (Ultra Alta Frecuencia), VHF (Muy Alta Frecuencia), HF (Alta Frecuencia), MF (Frecuencia Media), LF (Baja Frecuencia) y cubren el espectro desde 0 Hz (señal continua) hasta el límite con las microondas.
Tanto las microondas como las señales infrarrojas son todas ondas electromagnéticas, sólo que de diferentes frecuencias, lo que las hace aptas para múltiples usos.
Se puede demostrar que para que una onda electromagnética se propague, no es necesario contar con un medio (como las ondas sonoras) ya que lo hacen incluso en el vacío. La distancia física de la onda que se corresponde con un ciclo de la misma, se define como longitud de onda , su unidad es el metro (m), sus múltiplos y submúltiplos y tiene una relación inversa con la frecuencia, según la fórmula:

$$f = \frac{c}{\lambda}$$

Donde es la frecuencia en Hertz (Hz), es la longitud de onda, y es la velocidad de las ondas electromagnéticas en el vacío.

Mayor es la frecuencia, menor la longitud de onda. Así se habla de onda milimétricas, kilométricas, etc. Se puede demostrar que cuanto mayor es la frecuencia (menor longitud de onda), la onda tiene un mayor problema para atravesar objetos comparables con su longitud debido a la absorción de la energía puesta en juego en la onda. ¿Cómo es esto?
Cuando una onda se encuentra con un objeto, su energía hará vibrar los átomos del mismo, éstos absorberán parte de dicha energía asociada con la onda y el resto logrará atravesarlo.
Si la onda se encuentra con un objeto cuyo tamaño es comparable a su longitud de onda, mayor todavía será la absorción. Es decir, mayor es el objeto, más cantidad de átomos absorbentes y menor es la energía que propagará la onda que logre atravesarlo. Éste es el motivo por el cual a ciertas frecuencias se deba transmitir con las antenas ubicadas libres de obstáculos intermedios.

Esta misma razón es la que hace que los dispositivos que operan con la radiación infrarroja deban operar a corta distancia y sin obstáculos intermedios manteniéndose alineados respecto al receptor.
Pero esto no es todo, debemos mencionar que existen antenas que irradian energía en todas las direcciones (omnidireccionales) y aquellas que la concentran en una única dirección (direccionales).

Leonardo Becchio

Wireless: el futuro

(Wi-Max, Mobile-Fi, ZigBee y Ultrawideband)

Aún hoy, existen localidades remotas que no pueden gozar de las tecnologías tradicionales de banda ancha para tener acceso a Internet. Causa fundamental: el costo.

Pero esto está por cambiar. Por ejemplo el gigante inglés de las telecomunicaciones British Telecom (BT) ha invitado a 100 usuarios de un pueblito en Irlanda del Norte y de otras áreas rurales interesados en la web a probar las nuevas y prometedoras tecnologías del futuro cercano. BT ha instalado una serie de torres de transmisión de radio que emiten señales por toda la región a pequeñas antenas a los costados de las casas de los clientes. La conexión será tan veloz como banda ancha actual pero muchísimo más económica. ¿Por qué? Porque se utiliza equipo mucho menos costoso y un pedazo del espectro electromagnético (en la región de las ondas de radio) que no debe pagar licencias. De esta manera se evitan millones en pago de fees. Si el experimento resulta exitoso BT impondrá el año próximo este tipo de tecnología todo a lo largo y ancho de Gran Bretaña. “Esto revolucionará a la sociedad, del mismo modo que la telefonía móvil revolucionó a la sociedad en los años 80”, dijo Mike Galvin, el director de Operaciones de Internet en BT.

¿Es esto todo? No, esto es sólo un ejemplo de como la porción sin licenciar del espectro de radio se está transformando en algo muy pero muy especial. Durante muchos años estas frecuencias de radio fueron tomadas sin interés, dejadas para los teléfonos inalámbricos de las casas y los aparatos de microondas. Pero en los últimos años ingenieros del MIT y Phillips han estado trabajando en tecnologías basadas en este pequeño ancho de banda del espectro de radio. Estos estudios han sido los que lograron implementar la tecnología WiFi que actualmente domina todo lo que sea conectividad de redes wireless. Pero WiFi es sólo un pequeño escalón de las que serán 4 tecnologías innovadoras: Wi-Max, Mobile-Fi, ZigBee y Ultrawideband (Ultra Banda Ancha). Estas 4 tecnologías llevaran el networking inalámbrico a todas las facetas de nuestra vida diaria. Desde autos y hogares a edificios de oficinas y fabricas. Estas nuevas tecnologías ya han atraído en los últimos cinco años 4.500 millones de U$ en capitales de riesgo.

Los productos basados en ellas estarán ya disponibles durante 2005. Harán que Internet se expanda creando la posibilidad de conectividad en cualquier parte y en cualquier momento. Se contará con herramientas que permitirán la resolución de todo tipo de problemas ya sea conectividad dentro de un radio de unos pocos centímetros a kilómetros.

Una nueva era para la Web inalámbrica comienza. Estas tecnologías trabajaran entre si y con las tradicionales tecnologías de la telefonía celular permitiendo que gente y máquinas puedan comunicarse entre sí. Pequeños pueblos podrán tener conexiones de red muy veloces. Viajando por autopistas podremos conectarnos usando laptops o PDAs para chequear el clima o cómo está el tráfico en la ruta. En los hogares podremos ver películas captándolas de antenas parabólicas con las computadoras transfiriéndolas a nuestras TVs con pantallas planas. Todo esto SIN CABLES. Y, pequeños sensores ubicados en rascacielos controlarán las luces, y hasta podrán hacer un monitoreo de los niveles de toxicidad del agua de los desagües. Llegará a lo que se llamara el “Internet de los objetos”, donde máquinas inteligentes se comunicarán entre sí para decidir acciones que deberán tomar.”

¿Cuáles son entonces estas tecnologías de futuro cercano? ZigBee por ejemplo, con su tecnología estándar de radio coordinará la comunicación entre miles de pequeños sensores. Estos sensores estarán distribuidos entre oficinas granjas, o fábricas levantando información como temperatura, químicos, agua o aún movimiento. Estarán diseñados para consumir muy poca energía ya que deberán permanecer en su lugar por diez años. Así, se comunicarán muy eficientemente pasando la información a través de las ondas de radio como si pasásemos agua a través de baldes. Al final del camino los datos podrán ser dejados en una computadora para ser analizados o levantados por otra tecnología como WiMax. Productos que utilicen ZigBee ya aparecerán en el mercado a fin de año.

Enormes Puntos de Acceso Calientes (Hot Spots)

Wi-Max y WiFi son de algún modo similares. Para ambos se crean los llamados hot spots (puntos de acceso calientes) o áreas alrededor de una antena central donde la gente de forma inalámbrica puede compartir información o acceder a la Internet con una laptop apropiada. Mientras que WiFi puede cubrir unos 100 metros WIMax tiene un rango de los 50 Km. Esto es, puede reemplazar las actuales conexiones de banda ancha que utilizan líneas telefónicas y cable. Es justamente una versión de prueba de Wi-Max la que usara BT en Irlanda. Wi-Max aun no puede ser usada si se está en movimiento (por ejemplo en un auto). Pero aquellos que están atrás de la tecnología (como Intel y Alcatel) planean tener una versión móvil en pocos años. Un estándar similar, Mobile-Fi estará disponible en 2 o 3 años. Esto permitirá conexiones más veloces que las actuales de banda ancha y realizados desde autos o trenes.



Finalmente Ultrawideband. Esta tecnología sirve para otro propósito. Permitirá a la gente mover archivos enormes de modo muy rápido sobre distancias cortas. Esto permitirá llevar programas enteros en el hogar (por ejemplo de TV) desde la PC a la TV sin utilizar cables de ningún tipo. En la ruta un conductor que reciba en su baúl, con su laptop, información usando Mobile-Fi podría usar Ultrawideband para llevar esa información a su computadora de mano en el asiento delantero. Aunque el estándar no esta terminado Motorola ya esta vendiendo chips con esta tecnología.

¿Qué hace a estas tecnologías tan atractivas? Una es la naturaleza NO LICENCIADA de un pedazo de espectro de radio. Normalmente gigantes como AT&T pagan al gobierno enormes cantidades de dinero para poder operar en frecuencias de radio especiales. Esto permitió poder proveerle a sus cliente telefonía celular sin interferencia, pero bloqueaba a otros de utilizar dicha frecuencia. Todas las nuevas tecnología están basadas en el la parte del espectro NO LICENCIADA.

WiFi sentó el precedente de éxito que estas nuevas tecnologías intentarán imitar. Un grupo de empresas se unieron para definir el estándar WiFi iniciando un círculo virtuoso. Altos volúmenes de venta bajaron los precios del equipamiento, los bajos costos abrieron la demanda y la gran demanda llevó a volúmenes de venta más grandes aún. Ahora por ejemplo INTEL que comenzó el ciclo con unos 400 millones de U$, vende chips Wi-Fi a fabricantes de computadoras por U$ 20 cada uno. Un año antes se vendían a U$45. Unas 54 millones de laptops, PDAs y otros dispositivos Wi-Fi serán vendidos este año.

Todas estas tecnologías deberán vencer varios desafíos si desean imponerse. Los gigantes aun debaten sobre los estándares de Mobile-Fi y Ultrawideband y será recién en 2006 cuando quedarán definidos. Hasta entonces quienes fabriquen equipos no podrán comenzar producciones en masa lo que no permitirá baja de precios. Mobile-Fi está planeada para el espectro licenciado, podría no triunfar si se logra agregar capacidades de movilidad a Wi-Max.

¿Y qué pasa con la competencia?. Por ejemplo las compañías de celulares están sacando una tecnología que les permitirá a sus clientes tener conexiones de RED en sus teléfonos móviles y laptops. Esta, llamada 3era generación, o 3G, competirá directamente con WiMax y Mobile-Fi. Ya hay empresas que han instalado esta tecnología en áreas de Washington y San Diego en USA, Europa y Asia. La tecnología 3G puede ser más lenta que Wi-Max pero es muy confiable y ya disponible.

Aun si WiMax y las otras logran triunfar hay otro desafío: una escasez de espectro de frecuencias. Todas ellas usando el mismo espectro podrían llegar a interferirse. Para evitar tal problema empresas como Intel, Microsoft y otras están haciendo lobby a la FCC (Federal Communications Comisión) para más espectro. ¿Su meta? Los grandes emisores de TV incluyendo ABC, NBC, y CBS que están sentados sobre grandes cantidades de espectro para transmitir programas de TV. La FCC ha estado promoviendo el uso del espectro sin licenciar pero no es claro que quiera entrar en conflicto con las grandes emisoras de TV.

AUTOMATIZACION

Una de las razones de optimismo es que estas tecnologías podrán ofrecer beneficios de modo de hacer un shock en la economía. Internet wireless promete elevar la productividad colectando información que no podía registrarse anteriormente y haciendo que esta información esté disponible cuando se la necesite. Esto acelera la automatización. Ejemplo: que un cajero haga tareas mas productivas que solamente sentarse a registrar los productos de cliente. Ya Wi-Fi es usado por grandes tiendas de USA para inventarios y precios. Ahora la tecnología se esta moviendo a la construcción, servicios de rescate, salud y otros mercados. Se espera que combinadas, estas tecnologías lleguen a 17.000 millones en ventas en 2007 de 3.300 millones del 2003. La próxima ola de productividad personal en el trabajo tiene que ver con movilidad. Las personas queriendo tener acceso desde cualquier parte.

Hay signos de mucho interés en estas tecnologías: Andover Controls Corp que posee 100.000 sistemas de control de edificios instalados en el mundo trabajó junto a Goodman Manufacturing Co para bajar el gasto energético en un 10% con sensores ZigBee. En un test realizado se pusieron 4 sensores del tamaño de una caja de fósforos en cerca de 25 cuartos de hotel en Texas. Uno puesto en el aire acondicionado. Otros en las paredes para monitorear movimiento y temperatura en el cuarto.

Los sensores detectan si el aire acondicionado esta prendido. Luego una computadora central analiza la información y decide que acción tomar.

Las aplicaciones de esta tecnologías pueden ser aun mas ambiciosas. Por ejemplo, el departamento de energía de US ha contratado a Honeywell International Inc para usar sensores Zig-bee para ayudar a bajar costos de energía en un 15% en las industrias del acero, aluminio y otras seis. A modo de prueba estos sensores se instalarán este año en empresas como Alcoa, ExxonMobil, para monitorear pérdidas de energía de las cañerías y el uso de gases en los procesos de producción.

Estos procesos usan grandes cantidades de calor y energía para transformar gases como hidrocarburos en etileno que se usa para fabricar plásticos. Los sensores de Honeywell harán un seguimiento continuo de la cantidad de gas utilizado. Esto será muy diferente a la evaluación que se hace una vez al día hoy. Esto permitirá a las compañías eliminar perdidas o malgasto inmediatamente. Se estima que estas tecnologías wireless ayudarán a ahorrar 256 trillones de Btu de energía al año. Esto es más de la energía que utiliza una ciudad como Washington DC en un año.

Como las investigaciones continúan los sensores serán más pequeños y más versátiles. Eventualmente se espera llegarán a ser tan diminutos como del tamaño

▶▷

de las partículas de polvo. Miles de estos pequeños sensores o "smart dust" (polvo inteligente) podrían liberarse en la atmósfera para chequear cosas que van desde armas químicas a cambios climáticos.
Una vez que comiencen a integrarse, estas tecnologías permitirán otras innovaciones. Se espera que teléfonos celulares y laptop podrán cambiar el tipo de tecnología usada saltando de Wi-Fi a Wi-Max o la red tradicional telefónica. Por ejemplo los fabricantes de telefonía celular (Nokia, LG, Samsung) están incorporando tecnología Wi-Fi este año. Se esperan entonces nuevos servicios. Por ejemplo un proveedor de electricidad podría ofrecer descuentos a aquellos que utilicen sensores Zig Bee para monitorear su uso de electricidad con precios diferentes dependiendo de la demanda.
Hoy, ya universidades y varias empresas envían sus llamadas telefónicas sobre Wi-Fi. Dartmouth College en USA tiene una red WiFi sobre su campus y permite a los estudiantes hacer llamadas domésticas gratis usando sus laptops. Ahora están probando video wireless con la idea de ofrecer programación de TV-por cable sobre Wi-Fi. Este será pago para los estudiantes pero ahorrará ya que no habrá que mantener tres diferentes redes: cable, teléfono y servicio de RED.
Después de su éxito con WiFi, Intel intentará lo mismo con Wi-Max. Un MODEM Wi-Max costará U$ 450 que es mas que los U$ 50 de un MODEM banda ancha o los U$200 de una tarjeta de telefonía 3G. Pero se espera que Wi-Max dará velocidades de 5-10Mbits por segundo que es muchísimo mas que los 3Mbit por segundo de banda ancha o 300 a 5000 kilo bits por segundo de 3G. Tanto Intel, Siemens, Alcatel, y Motorota han anunciado que incorporaran Wi-Max a sus productos y creen que van a lograr atraer mercado y lograr bajar los precios. Muchos parecen aun proyectos e ideas en desarrollo. Pero, eso es lo que flota en el ambiente y paso a paso se va concretando.

WI-MAX

En el auge de las tecnologías Wi-Fi y Bluetooth aparece un nuevo estándar denominado **WI-MAX** enmarcado en el estándar IEEE 802.16. **WI-MAX**, por **W**orldwide **I**nteroperability for **M**icrowave **A**ccess (la **X**, resulta de la semejanza en la fonética de la palabra *access*) es una nueva tecnología que permitiría entre otras cosas interconectar ciudades en forma inalámbrica mediante un enlace por radiofrecuencia. Uno se estará preguntando seguramente en qué se diferencia de Wi-Fi y de Bluetooth. Cuidado, no se confunda. Bluetooth se utiliza básicamente para interconectar dispositivos en un radio de aproximadamente 10 metros. Wi-Fi se lo utiliza para la interconexión de dispositivos en un radio un poco mayor, los 100 metros, de modo de poder armar una red de área local inalámbrica, WLAN.
Por otra parte **WI-MAX** promete la comunicación a distancias mayores de modo de poder armar lo que se denomina una red de área amplia o WAN.
El estándar IEEE 802.16 especifica una arquitectura punto a multipunto (uno transmite, muchos reciben) operando entre los 2 GHz y los 66 GHz abarcando tanto especificaciones para la capa de enlace de datos (capa 2 del modelo OSI) como para la capa física (capa 1).
flexiblemente para transportar cualquier tipo de encapsulado tales como Ethernet, IP y ATM.

El Wi-Fi del futuro (Wi-Max) tendrá un alcance mucho más largo

Nick Wingfield en el The Wall Street Journal escribió un excelente artículo sobre Wi-Max y su relación con Wi-Fi. A continuación le damos un resumen de los puntos más sobresalientes.
Que se quite el Wi-Fi; aquí viene el Wi-Max. En solo unos años, la popular tecnología conocida como Wi-Fi ha dado a millones de computadoras acceso inalámbrico a Internet a velocidades de banda ancha en oficinas, casas y cafés.
Pero el equipo Wi-Fi tiene una limitación; está hecho para dar acceso inalámbrico en una circunferencia de solo 100 metros de un transmisor de radio conectado a una conexión de Internet de banda ancha. Esto no sirve para crear acceso de banda ancha en las zonas rurales que no tienen cable o servicios de DSL y en zonas en las que esos servicios no funcionan bien. Y significa que no se puede abrir la computadora en cualquier parte y estar conectado a Internet. Ahora existe una tecnología llamada WiMax que promete liberar el acceso inalámbrico a Internet de esas limitaciones. Las antenas WiMax serán capaces de transmitir conexiones de alta velocidad para Internet a casas y negocios que se encuentran a kilómetros de distancia, lo que eliminaría la necesidad de que cada edificio tenga que estar cableado para acceder a Internet. Pasara algún tiempo antes de que el WiMax tenga que demostrar su potencial real: no se espera que la tecnología este disponible de forma amplia hasta los alrededores de 2006.Pero un creciente números de empresas, entre ellas Intel Corp., el fabricante de chips de Santa Clara, California, cree que el WiMax desencadenará una ola de compras en tecnologías inalámbricas.Al enviar sus señales sobre áreas metropolitanas enteras y más allá, WiMax permitirá verdadera movilidad inalámbrica, es decir, la capacidad de utilizar una computadora portátil para acceder a Internet desde todas partes y no solo en los puntos definidos donde las antenas Wi-Fi ofrecen actualmente ese acceso.
Para los aficionados al acceso móvil de Internet, será como cambiar un teléfono fijo inalámbrico por uno celular, aunque pasaran años, si acaso, antes de que el alcance de WiMax se asemeje al de las redes de telefonía celular.

RFID

Radio frequency identification (**RFID**) es un método para almacenar y obtener datos en forma remota usando dispositivos llamados RFID tags (etiquetas RFID). Un RFID tag es un objeto de dimensiones pequeñas (como una etiqueta adhesiva) que puede ser adherido o incorporado en un producto. Los RFID tags contienen antenas para permitirles recibir y responder lo enviado por un transceiver (ver **que es un transceiver?**) RFID utilizando radio frecuencia.

Tipos de tags RFID.

Los tags RFID pueden ser activos o pasivos. Los tags RFID pasivos no tienen su propia fuente de alimentación: la minúscula corriente eléctrica inducida en su antena por las ondas electromagnéticas que envia el transceiver dan potencia suficiente para que el tag haga una respuesta. Debido a la energía consumida y costos, la respuesta de un tag RFID es necesariamente breve, típicamente solo un número identificatorio (ID number) (GUID: Globally Unique Identifier). El no tener su propia fuente de alimentación hace que sean muy diminutos: existen productos comerciales que hasta pueden ser instalados debajo de la piel. Tags RFID activos, por otro lado, tienen una fuente de alimentación, y pueden tener alcances más grandes y memorias mas grandes. Por ende pueden almacenar mas información enviada por el transceiver. Como los tags pasivos son mas económicos de fabricar, la mayoría de los tags RFID son del tipo pasivo. Existen cuatro tipos diferentes de tags usados comúnmente. Su diferencia se basa en la frecuencia de radio utilizada: tags Low frequency (entre 125 a 134 kilohertz), tags High frequency (13.56 megahertz), tags UHF (868 a 956 megahertz), y tags Microwave (microondas) (2.45 gigahertz).

Usos más frecuentes

Los tags RFID de Low-frequency son usados comúnmente para identificación de animales, para tracking de barriles de cerveza, en llaves y locks antirrobos de automóviles. Tags RFID High-frequency se utilizan en bibliotecas o librerías para busqueda de libros, tracking de bultos, acceso a edificios, tracking de equipaje en aeropuertos. Son también muy usados en distintivos identificadores reemplazando tarjetas magnéticas. Estos deben ser aproximados a una distancia corta de los lectores para poder identificar al poseedor. Tags RFID UHF son usados comercialmente en tracking de contenedores, camiones y acoplados en depósitos.Tags RFID Microwave (microondas) control de acceso de automóviles de largo alcance.Algunos peajes están equipados para leer tags RFID cuando pasan los vehículos. El tag está asociado a una cuenta prepaga de la cual se debita el costo.Algunos tipos de sensores, como sensores sísmicos, pueden ser leídos usando transceivers RFID lo que simplifica enormemente la recolección de datos.En 2003 Michelin anuncio que comenzó a probar transponders RFID embebidos en cubiertas. El propósito será finalmente conocer el estado de las cubiertas para conformar las leyes vigentes.

Usos potenciales

Los tags RFID se ven como reemplazo del código de barras UPC (Universal Product Code) teniendo un número importante de ventajas. Los códigos RFID son suficientemente grandes para poder dar un único código a cada producto mientras que los códigos de barra son idénticos para todas las instancias de un mismo producto. Esto significa que el producto puede ser monitoreado individualmente mientras se mueve de lugar en lugar, finalmente terminando en manos del cliente final. Esto permitirá a las empresas combatir los robos y otras formas de pérdidas de productos. Ha sido también propuesto como punto de venta en tiendas de modo de reemplazar a los cajeros con un sistema automatizado. A la salida se descontaría de una tarjeta de crédito o insertando dinero en una maquina de pago.Hasta se habla de usos como permitir a las heladeras monitorear los productos de nuestra casa dándonos la información de los faltante.

Controversia

El uso de la tecnologías RFID ha generado alguna controversia. Lo más preocupante es el hecho que estos tags seguirían pegados a los productos llevados al hogar. Aunque los tags son oficialmente preparados para usar en cortas distancias, pueden ser interrogados desde lejos si se posee una antena apropiada. Esto permitiría que los contenidos de una casa podrían monitorearse a distancia.

Los cuestionamientos mas graves :

El que compra un producto no estará necesariamente alerta sobre la presencia del tag o ser capaz de removerlo

El tag se puede leer a distancia sin que lo sepa el individuo

Si el producto se paga con tarjeta de crédito se podría en principio asociar el ID de ese producto a la identidad del comprador.

¿Qué es un Transceiver?

En networks de computadoras, el término transceiver es un dispositivo que realiza, dentro de un chasis, funciones de transmisión y recepción en un solo dispositivo. Muchas veces son diseñados para uso de equipos portátiles o móviles. Utilizan componentes electrónicos comunes para ambas tareas: transmisión y recepción lo que da operación "half duplex".

Los transceivers fueron usados muy comúnmente en redes ethernet 10BASE5.

En electrónica, el termino transceiver se refiere a un dispositivo que combina transmisión y recepción en un mismo empaquetamiento. Ejemplos: walkie-talkie o una radio CB (Citizen Band radios).





¿QUÉ SIGNIFICA VPN?

Un "Virtual Private Network" (VPN) es un network (red) de datos privados que utiliza l a infraestructura de telecomunicaciones pública, manteniendo la privacidad a través de protocolos de túneles y procedimientos de seguridad.
Una VPN puede ser contrarestada con un sistema de líneas propietarias o bajo leasing, que sólo pueden ser usadas por una compañía. La VPN brinda a una empresa las mismas posibilidades que las líneas privadas bajo leasing a un costo muchísimo más bajo, utilizando la infraestructura pública compartida (un ejemplo: Internet).
Bajo las siglas VPN se reúne un conjunto de tecnologías y escenarios para satisfacer las necesidades de las empresas.

Cuando se selecciona una implementación VPN se deben considerar: seguridad, interoperabilidad, facilidad de uso y administración.

Existen soluciones VPN provistas por diferentes vendors pero también existen soluciones gratis disponibles en diferentes sistemas operativos (SO). O soluciones que si no están ya en el SO pueden bajarse de Internet.

En este artículo se discute la tecnología VPN en su forma genérica. Independientemente de cómo se las implementa. Es necesario adentrarse en los siguientes puntos:

*Protocolos disponibles (PPTP / L2TP / Ipsec / IPsec Túnel)
*Escenarios VPNs más comunes (Acceso remoto, site-to-site, extranet)
*Autenticaciones
*Seguridad bajo VPN
*Interoperabilidad de VPN entre Linux y MS

En el caso Windows, si nos referimos a un servidor VPN se deberá entender Windows 2000 Server o Windows.NET Server 2003 con RRAS (Routing and Remote Access) activado.

VPNs y Acceso Remoto (remote Access Vpn) Figura 1:

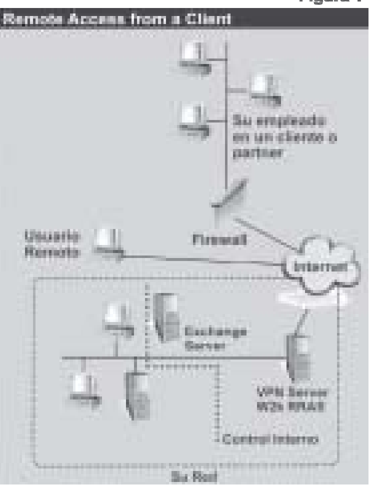
La mayoría de las compañías necesitan proveer Acceso remoto a los empleados. Generalmente se utilizaba una conexión dial-up (DUN) del cliente al servidor de acceso remoto (RAS) vía módems.
Para acceso remoto VPN hay que considerar: tecnología en la Workstation cliente, qué sucede en el medio entre el cliente y el servidor VPN, el servidor VPN y finalmente la relación con el usuario remoto.
El usuario remoto puede ser un empleado o individuo de menor confianza (un consultor a partner de negocios). Usualmente, el cliente de la Workstation estará corriendo bajo el SO Windows, pero podrá ser una estación MAC, Linux o Unix.

Una VPN es una red privada que usa una infraestructura pública manteniendo privacidad por medio de túneles y procedimientos de seguridad

SOs' pre-W2K y Workstation que no sean Microsoft imponen algunas limitaciones sobre los tipos de protocolos VPN y autenticaciones que se pueden usar. Para SOs pre-Win2k se pueden eliminar algunas de esta limitaciones haciendo un download desde Microsoft.
Cómo accede el usuario remoto al VPN server vía Internet no es de importancia. Sí, recordar que el ancho de banda deberá ser apropiado para que la conexión tenga sentido. Normalmente los proveedores de Internet (ISP) no bloquean los protocolos que se utilizan. Sólo puede haber problemas en el caso de que el usuario remoto trate de conectarse al VPN server (vía Internet) desde dentro de una red (un empleado visitando un cliente o proveedor) y deba pasar un firewall. Para este tipo de situaciones, una solución es un http-tunnel, como el propuesto e www.http-tunnel.com, que permite llegar a Internet vía el puerto 80 de http y entonces establecer el túnel VPN.

Una vez que el usuario remoto "disca" al número IP del servidor VPN se ingresa a la etapa de autenticación y autorización. Básicamente: ¿quién es usted?: Nombre de usuario y password y luego, ¿de qué modo lo autorizo a entrar en la red? (horario, protocolo).Toda ésta infraestructura deberá ser configurara por el administrador para garantizar seguridad.
Según el protocolo en uso y el SO en el servidor VPN y usuario remoto, existirán diferentes modos de autenticar (passwords tradicionales, certificados de usuario, tokens o biométrica).
Finalmente si se desea que el usuario remoto pueda acceder a la Intranet o si se lo limitará a áreas específicas. Se puede implementar esta "restricción" de diferentes modos: en el Server VPN, en los routers, o en las workstations y servers usando IPSec y políticas asociadas. En servidores VPN con W2K existe la posibilidad de usar Remote Acceses Policies (RAP).
En W2K uno puede por ejemplo restringir a usuarios o grupos de usuarios en el servidor VPN un grupo local o de dominio. Por ejemplo, si un consultant de Oracle entra en Intranet, ¿cómo se restringe el acceso al servidor correspondiente? Se crea un grupo, llamándolo Oracle Consultants, y se agregan las cuentas de usuarios. Entonces mediante la consola (MMC) de Routing and Remote Access (RRAS) se agrega una política de acceso remoto, se lo *linkea* al grupo Consultants y se agrega un filtro IP a la política que limite el tráfico del usuario remoto a destino, el servidor Oracle.

Figura 1



SITE-TO-SITE VPN (VPN entre sitios) Figura 2:

Todo lo que se necesita es un servidor W2K en cada sitio conectado a la LAN local. Este escenario no requiere autenticación de usuario pero sí deben autenticarse los servidores VPN entre sí.

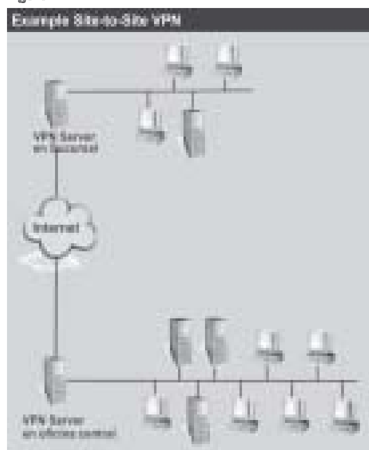
Existen soluciones VPNs provistas por vendors pero también las hay gratis incluídas en diferentes SO

Cuando se establece la conexión VPN, uno de los servidores VPN asume el rol de cliente e inicia una conexión con otro servidor VPN. Después de establecida la conexión VPN, los usuarios de cada sitio puede conectarse a los servidores como si estuvieran en la misma red local.
¿Cómo saben los servidores VPN que cada uno es auténtico y no un impostor? De acuerdo con el protocolo y el SO instalado en los servidores VPN, se puede basar la autenticación site-to-site en contraseñas asociadas con cuentas de usuario creadas para cada servidor, en llaves secretas pre-acordadas o en certificados para cada máquina emitidos por una autoridad certificadora (CA, Certificate Authority).

EXTRANET VPN (Figura 2 con control interno)

Permite conectar la red de una empresa con uno o más "partners". Este escenario es muy similar a site-to-site aunque existen pequeñas diferencias. Básicamente la confianza entre ambas partes es diferente. Se permitirá a una sucursal acceder a todos los recursos de la red corporativa (site-to-site), pero es posible limitarlos para un partner. Normalmente se los restringirá a sólo unos cuantos servidores de la red. Con el tipo de restricción ya descriptos en Remote Access, podemos solucionar el problema.
La segunda diferencia con site-to-site es que muy probablemente nuestro "partner" use una solución VPN diferente. Aparece aquí un problema de interoperabilidad a resolver. Para ello, se deberá atender, por ejemplo, a qué protocolos se usan en ambas soluciones VPNs y a qué tipo de autenticación se usará.

Figura 2



Suplemento Seguridad

Microsoft®

Ethical Hacking

Todo sobre Null Sessions o Login anónimo

El tema seguridad es hoy una prioridad para aquellos que utilizan sus sistemas informáticos estando interconectados en red y/o accediendo a la "red de redes" (internet). ¿Qué podemos hacer para que nuestros sistemas sean un poco más difíciles de hackear?

Mucho se puede hacer instalando los parches (patches) de seguridad de Microsoft, que tapan algunos huecos dejados inadvertidamente en la seguridad de los sistemas operativos al momento de su lanzamiento. En la mayoría de los casos la pregunta de ¿debería tapar este hueco? es bastante facil de responder. Pero hoy vamos a hablar de uno que puede ser bastante peligroso, aunque debemos ser muy cuidadosos con él porque cerrarlo puede crear problemas (hacer que deje de funcionar algo). Sin embargo es algo que todos deberían examinar. Estamos hablando de algo llamado "Null Session"; está también referido a login anónimo, y en realidad no es un "hueco en la seguridad" (security hole), es más bien una "característica" (no confundir con login anónimo a servidores FTP, eso es algo totalmente distinto).

¿Qué es una null session? ¿Qué puede hacer?

Una null session es una conexión de login establecida sin credenciales. Sí, asi es, una vasta mayoría de sistemas NT 4, W2K, W XP y W 2003 permiten que la gente se loguee sin proveer un nombre de usuario y una clave. Las null sessions o logins anónimos son preocupantes porque, por defecto, permiten que *cualquiera se meta en un dominio NT4 o en un Active Directory basado en W2K y obtenga acceso a cosas como:*

-La lista de usuarios de la SAM del sistema
-Los SIDs de las cuentas de usuario y convertir los SIDs en nombres de usuarios
-La lista de maquinas del dominio
-Las políticas de passwords y bloqueos de usuarios del sistema o del dominio
-El nombre NetBIOS de la máquina y el nombre del dominio al que pertenece
-La lista de grupos de la SAM
-Los dominios en los que su dominio confía

¿Pero, cuál es el peligro de esto?, en realidad no hay un daño inmediato o directo, ya que las null sessions no pueden capturar passwords. Pero mientras más conozca un hacker, mas fácil es para él ingresar al sistema. En teoría alguien podría obtener los nombres de usuario y utilizar un programa de fuerza bruta probando infinidad de passwords con cada uno. Eso puede llevarle mucho tiempo, es cierto, y también lo es que posiblemente usted note algo raro en los logs de seguridad al ver que el usuario Juan34 tuvo cinco millones de logins fallidos en los últimos dos días. Y si hay seteado un máximo de logins fallidos en su sistema, entonces el atacante (cracker o kiddie, en este caso) podría intentar passwords incorrectos adrede, dejando de esa manera bloqueados a todos los usuarios del sistema, la única solución a eso sería que el administrador desbloqueara a todos los usuarios, pero sólo lo puede hacer desde un controlador de dominio. Asi que dejar que cualquiera vea la lista de usuarios, probablemente no sea una buena idea.

Otra vez, vamos a dejarlo claro: CUALQUIERA puede establecer una null session. No necesita tener una cuenta en su dominio. Ni siquiera tiene que ver con la cuenta guest o invitado, las null sessions se pueden establecer aún si esas cuentas están deshabilitadas.

Una null session de ejemplo

¿Qué dice? ¿qué quiere probar? Primero que nada: no intente esto en la red de otra persona. Puede no ser legal. Y posiblemente tampoco deba probarlo en la red de su empresa, a menos que esté autorizado a testear la seguridad de la red. Lo mejor es probarlo en una red en la que tenga permiso para hackear, una red con propósitos de testeo, por ejemplo.

Se comienza con dos sistemas: víctima y villano. La víctima puede ser una estación de trabajo o un Controlador de Dominio. Se verán resultados diferentes en ambos casos y es interesante probarlo con los dos. También se verán grandes diferencias de comportamiento entre NT 4, 2000, XP y 2003.

Recuerde que queremos similar una situación donde víctima y villano normalmente no se comunicarían entre si, asi que asegúrese que:

Víctima y villano no están en el mismo dominio
El nombre de usuario y password que está usando en villano no es igual a un nombre de usuario y passwords válidos en víctima; por ejemplo, si está usando el usuario administrador en villano, asegúrese de que la cuenta administrador de víctima no tenga la misma clave. Si fuera así, entonces villano usaría automáticamente ese hecho para loguearse a víctima, arruinando asi todo el propósito de explorar los alcances de una null session.

Asumiendo que villano puede resolver el nombre "víctima" pruebe lo siguiente

net view \\victima

Note la sintaxis, se sigue el uso normal del comando NET USE con /u:"" seguido de un espacio y "" (otro par de comillas). Esto significa "logueame con un nombre de usuario vacío y una clave vacía", la caracteristica del Usuario Anónimo. Probablemente vea la respuesta "Comando completado exitosamente", lo que significa que se estableció una null session o login anónimo. Si, por el contratrio, ve un mensaje como "System error 5" quiere decir que alguién aseguró a víctima de alguna manera contra logins anónimos, ¡¡felicitaciones!!.

(nota: sin haber creado una null session, pruebe: net view /domain:*nombredominio . Por alguna razón parece funcionar siempre, no importa cuanto se restrinja el uso de null sessions, raro. Aparentemente cualquiera puede obtener una lista de las máquinas de un dominio).*

(nota: en Windows Server uno encuentra varios "shares"(recursos para compartir) que fueron creados sin nuestra intervención). La mayoría de estos shares son "hidden" (ocultos) y se los nombra con $ al final. Ejemplos: C$.D$, ADMIN$.

...el atacante hacker intentando passwords incorrectos puede bloquear a los usuarios del sistema.

(nota: el "share" IPC$ es quizás uno de los shares más usados en comunicacones entre servidores. ¿Cómo leemos los "event logs" en otra computadora, por ejemplo?. Uno no mapea un "drive" sino los llamados "named pipes": un pedazo de la memoria que maneja la comunicación entre procesos ya sean locales o remotos)

Asumiendo que ya estableció una null session, pruebe el comando "net view \\víctima", esto le dará la lista de "shares"(recursos compartidos) de esa computadora. Pero ¿qué más podemos ver?, bueno para explotar realmente lo que una null session nos puede dar necesitamos la herramienta multi-propósito para null sessions "enum.exe" que puede ser encontrada en http://razor.bindview.com/tools/desc/enum_readme.html.

Desafortunadamente está empaquetada en formato tar zipeado, un formato muy común en ambiente UNIX/Linux, para comprimir y transmitir grupos de archivos, pero no tan común dentro del mundo Windows. Se puede, sin embargo, abrirlo con alguna versión actual de PKZip. Dentro se encuentra un archivo llamado enum.exe, ese es el que necesita. Ejecútelo desde la línea de comandos para tratar de obtener la lista de usuarios, de máquinas en su grupo de trabajo, recursos compartidos, información de la política de claves, grupos y dominios confiables. Pruebe con la siguiente linea:

enum -U -M -S -P -G -L victima

Cuando se utiliza contra un sistema básico NT4 o 2000, enum obtiene una buena cantidad de información:

C:\>enum -U -M -S -P -G -L nt4basesystem
server: nt4basesystem
setting up session... success.
password policy:

▶▷

Este artículo fue extraído de: **Mark Minasi's Windows Networking Tech Page Issue #34 June 2003.** Recomendamos a aquellos que deseen encontrar material de excelente nivel sobre Windows 2000 y 2003 visitar la web page de Mark y suscribirse: **http://www.minasi.com**



Suplemento Seguridad

```
min length: none
min age: none
max age: 42 days
lockout threshold: none
lockout duration: 30 mins
lockout reset: 30 mins
opening lsa policy... success.
server role: 3 [primary (unknown)]
names:
 netbios: NT4BASESYSTEM
 domain: WORKGROUP
quota:
 paged pool limit: 33554432
 non paged pool limit: 1048576
 min work set size: 65536
 max work set size: 251658240
 pagefile limit: 0
 time limit: 0
trusted domains:
 indeterminate
netlogon done by a PDC server
getting user list (pass 1, index 0)... success, got 2.
 Administrator Guest
enumerating shares (pass 1)... got 5 shares, 0 left:
 ADMIN$ IPC$ stuff C$ Z$
getting machine list (pass 1, index 0)... success, got 0.
Group: Administrators
NT4BASESYSTEM\Administrator
(....)
```

Cuando se lo usa contra un XP o 2003 sin modificar, se obtiene mucha menos información un montón de mensajes de "acceso denegado".

En primer lugar: ¿porqué existen las null sessions?

La primera vez que leí sobre null sessions, en la época de NT4.0 SP3, me espanté. ¿Cuál es el punto de tener un sistema operativo seguro, con toda clase de listas de permisos -- incluyendo permiso de lectura -- , cuando el mismo simplemente ignora cualquier permiso existente y permite a cualquiera ver mis dominios por dentro?

La respuesta es que aparentemente, hace las cosas mucho mas fáciles para los programadores de Microsoft. El ejemplo clásico comprende 2 dominios NT4 con una relación de confianza simple de una vía, los llamaremos MAESTRO y RECURSO. RECURSO confía en MAESTRO pero MAESTRO no confía en RECURSO.

Ahora vamos a suponer que soy el administrador de RECURSO. Hay un grupo global en MAESTRO llamado VIAJANTES (MAESTRO\VIAJANTES, para decirlo correctamente) al que le quiero dar control total de un recurso compartido en un server de mi dominio. Asi que voy hasta ese server, abro la Access Control List (Lista de Control de Acceso ACL) de ese recurso compartido. Haglo click en "agregar" y quisiera elegir "MAESTRO/VIAJANTES" de una lista de grupos globales del dominio MAESTRO... ... y aqui es donde empieaza el problema. Recuerde que RECURSO confía en MAESTRO, pero no al revés. Asi que cuando el servidor en RECURSO en el cual estoy trabajando le pide a un Controlador de Dominio del dominio MAESTRO que le de una lista de grupos globales, el Controlador de Domino de MAESTRO, dice "¿si? ¿quién es que lo pide?" o, en idioma NT, "¿podría usted loguearse antes, de esa manera puedo saber si debo acceder o no a su pedido?", pero como MAESTRO no confía en RECURSO, el controlador de dominio de MAESTRO rechazará cualquier SID del dominio RECURSO, asi que será imposible para mi loguearme, y entonces será también imposible acceder a la lista de grupos globales.

La respuesta fue entonces setear a NT para que revele alguna información a cualquiera que se lo pida. Asi es como RECURSO obtiene la lista de usuarios globales de MAESTRO. Deshabilitar las null sessions veremos cómo en un momento hará imposible para el administrador de RECURSO acceder a los datos de MAESTRO.

(Pero aqui está la parte de las null session que me confunde. ¿Por qué crear ésta gigantesca puerta trasera(backdoor)? ¿por qué no, simplemente, modificar NT para que revele listas de grupos y usuarios a dominios confiables?, puede ser que se me esté escapando algo, pero esto parece una cosa asi como "son las 4 PM del viernes, ya compré los pasajes y me estoy yendo de vacaciones. Asi que relajo todo y chau". Mirar un problema de seguridad y decir simplemente "supongo que tenemos que aflojar un poco las cosas" no me razón para tirar por la borda la seguridad)

Incluso, no es éste el único caso de "necesito información, incluso aunque no me pueda loguear". Cualquier sistema con Windows 9x intentando acceder a la lista de equipos de un browse master basado en NT, 2000, XP o 2003 no tendría credenciales suficientes para hacerlo, y por eso sería incapaz de obtener la lista, de esa forma la lista de Network Neighborhood ("computadoras cerca mío") en ese sistema estaría vacía. Asi que Microsoft modificó la familia NT (NT 3.x, 4, 2000, XP y 2003) para permitir que usuarios anónimos con null sessions pudieran acceder a la lista de equipos. Si elige restringir el acceso de null sessions en su red, entonces el network neighbohood (vecindario de red equipos cerca mío) no funionará en ciertas situaciones, particularmente cuando intervengan (según algunos reportes) NT4 o win 9x revisando (browsing) un dominio. Ahora, eso puede atraer la atención de sus usuarios, peor aún, monotnes de aplicaciones han confiado durante años en la existencia de las listas de equipos. Los usuarios de BackupExec, por ejemplo, saben que esa aplicación les permite realizar backups de sistemas remotos se puede, desde Server1 realizar un backup de Server2 como si la unidad de cinta estuviera en Server2. Pero BackupExec 8.5 y anteriores fallarán completamente si tratan de hacer un backup de un sistema remoto que tenga deshabilitado el uso de null sessions.

Eso ha desembocado en que aquellos que quieran anular las null sessions deben dar extrañas vueltas para hacerlo. Un administrador de red solucionó el problema de tener vacia la lista de "equipos cerca mío" forzando a todos sus sistemas basados en NT (NT 4, 2000, XP, 2003) a NO SER browse masters, así sus sistemas basados en Win9x (los cuales les entregan a *cualquiera sus listas de equipos) se convirtieron en sus browse masters!!.*

Restringiendo las Null sessions

Mientras Windows se hacía popular, los hackers descubrieron las null sessions y las usaron para crear una variedad de molestas herramientas (la mas conocida es RedButton), que usa una null session para identificar el nombre de la cuenta Administrador, incluso si ha sido renombrada (aunque no crackea la clave). Por eso Microsoft cambio la familia NT de modo que uno pudiese restringir de algún modo el acceso de null sessions.

Cuales son estas posibilidades de restricción?:

Primero, está la "desaparición absoluta de null sessions": se bloquean los puertos 139 y 445. Las null sessions directamente no pueden existir sin ellos.

En NT 4 con Service Pack 3 o posterior, Microsoft agregó la entrada de registro RestrictAnonymous, de tipo REG_DWORD HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\LSA. Puede tener los valores 1 ó 0. 0 es el valor por defecto y deja al sistema en el estado original (relativamente abierto). Si se establece el valor de RestrictAnonymous en 1 y se resetea el equipo, nos encontraremos con un NT4 considerablemente menos generoso con la información para los visitantes anónimos; si se utiliza el enum.exe contra un equipo en ese estado se obtiene una muy pequeña cantidad de datos, no mucho. El comando NET USE funcionará con una null session, es decir vemos el mensaje "el comando se completó con éxito" pero solo obtenemos un mensaje de "acceso denegado" cuando realizamos peticiones sobre las recursos compartidos.

En Windows 2000 , Microsoft redefinió a RestrictAnonymous. Ahora los valores posibles son 0,1,2. En Windows 2000, 0 significa que no hay restricciones a las null sessions, como antes. Pero el 1 está redefinido. 2 significa lo que significaba el 1 antes (básicamente impide la mayoría de los accesos de las null sessions). El "nuevo 1", en contraste, solo evita que sean consultadas las listas de usuarios y de recursos compartidos.

Microsoft también muestra este registro a través de las Group Policies Mire en Computer Configuration / Windows Settings / Security Settings / Local Policies / Security Options y la primera entrada se llama: "restricciones adicionales en conexiones anónimas" y ofrece tres valores: "ninguna. Depender de los permisos originales", "No permitir enumeración de las cuentas SAM ni recursos compartidos" y "No permitir acceso sin permisos explícitos para usuarios anónimos". Se habrá dado cuenta de que se corresponden exactamente con los valores 0, 1 y 2 de la versión Windows 2000 de RestrictAnonymous.



VPN la solución para seguridad en redes inalámbricas usando W2K

Si en sus oficinas existe un AP (Access Point) wireless (inalámbrico), cualquiera con una laptop y el software apropiado puede asociarse a su red y así acceder a documentos confidenciales o mensajes de e-mail. Cualquiera puede sencillamente instalar un AP inalámbrico sin que usted (administrador) se entere, creando así un agujero en la seguridad de su red. A continuación veremos cómo podemos configurar APs usando las capacidades de seguridad que vienen del fabricante en conjunto con Microsoft Routing y Remote Access Service (RRAS). Así lograremos protegernos y disminuir los riesgos.

¿Qué viene por defecto como seguridad con la infraestructura inalámbrica?

Existe mucha documentación en Internet acerca de cómo asegurar una red inalámbrica usando nada más que el equipo que su fabricante le provee. Los procedimientos para hacerlo varían de fabricante en fabricante. Mencionemos las dos técnicas más comunes: Wire Equivalent Privacy (WEP) y listas de Media Access Control (MAC).

WEP (Wire Equivalent Privacy)

La infraestructura de encriptación que viene por defecto para redes inalámbricas ya hace tiempo que ha sido quebrada. Así se use un WEP de 40 bits o uno de 128, un intruso puede decodificar el código de WEP que usa para su red. Esto es seguramente muy llamativo pero aún más es saber del gran número de redes inalámbricas que ni siquiera usan WEP. Si realiza el ejercicio de explorar redes inalámbricas, encontrará muchos APs inalámbricos, y casi ninguno de ellos usarán la encriptación. La mayoría de la gente se toma su tiempo para nombrar a sus redes inalámbricas, simplificando todavía más la tarea de determinar quien está corriendo una red abierta. Muy probablemente usen el nombre que identifica a la empresa. Si no planea usar WEP, al menos debería evitar dar a su red un nombre descriptivo.

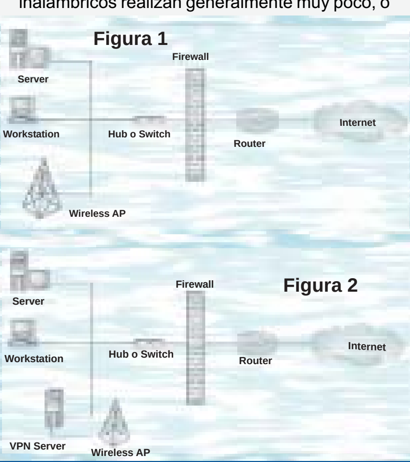
Aunque WEP ha sido quebrado, puede utilizarlo como punto de partida de seguridad para desalentar a la gente a procurar entrar a su red. Algunas revisiones más nuevas de equipos inalámbricos mejoran la seguridad de WEP, haciendo que su código de WEP sea mucho más difícil-sino imposible- de decodificar.

Listas de direcciones MAC

Algunos APs inalámbricos le permiten construir una tabla de direcciones de MAC autorizadas. Esta dirección MAC es única de cada NIC (*Network Interface Card*) inalámbrica. Si un NIC inalámbrico no autorizado intenta asociarse con su AP inalámbrico, el AP lo rechaza. Este paso extra toma un poco de esfuerzo ya que necesita agregar manualmente cada tarjeta a la tabla de MAC´s autorizados. Sin embargo, haciéndolo se le agrega una capa extra de seguridad a su implementación inalámbrica.

Seguridad

La causa fundamental de las deficiencias de las redes inalámbricas está en las áreas de autenticación y encriptación. Los APs inalámbricos realizan generalmente muy poco, o ninguna autenticación del usuario. Si el usuario se encuentra dentro del alcance de su AP y usted no esta usando ningún tipo de seguridad, el o ella se conecta a su red. WEP proporciona alguna mejora pero no es la solución final. La pregunta es: ¿qué clase de tecnología de redes puede darle autenticación a los usuarios que vienen de un espacio poco confiable y encriptar sus comunicaciones para que nadie pueda interceptarlos? La respuesta es VPN.Una VPN resuelve las deficiencias corrientes de las redes inalámbricas. Pero conectarse se vuelve





un poco más complejo para sus usuarios. Si ya invirtió tiempo en construir una infraestructura de VPN para que sus usuarios móviles accedan a la red de su organización a través de Internet instalar una VPN para autenticar usuarios wireless es relativamente fácil.

Vamos a mirar una red corporativa ficticia antes y después de usar un VPN para asegurar las conexiones inalámbricas. La figura 1 muestra un diagrama de red de una típica implementación inalámbrica, con el AP inalámbrico detrás del firewall de su corporación. En ésta configuración usted pudo haber gastado mucho dinero en equipos de firewall para mantener conexiones poco confiables fuera de la red, pero este tipo de implementación abre un gran agujero dentro del espacio confiable de la red. Es como poner candados en la puerta y dejar la ventana abierta.

La figura 2 muestra una forma segura de implementar un AP inalámbrico: detrás un servidor VPN. Ése tipo de implementación provee alta seguridad para la implementación de sus redes inalámbricas sin sumarle mayor dificultad a sus usuarios. Para una protección extra, puede probar moviendo el servidor de VPN al frente de su firewall, pero como los APs son típicamente dependientes de la distribución física, esta posibilidad no funcionará para todos.

Si usted tiene más de un AP inalámbrico en su organización, le recomiendo conectar a todos dentro de un mismo switch, y ahí conecte su servidor VPN. De este modo, sus usuarios de desktop, no necesitarán tener múltiples configuraciones dial-up. Ellos siempre estarán autenticando al mismo servidor VPN sin importar a cual AP inalámbrico estén asociados.

Instalación del servidor VPN

Vamos a hablar sobre el hardware que va a necesitar este proyecto. Primero, necesitará un servidor para actuar como su dispositivo de entrada VPN (Gateway VPN) y controlar quién entra a su red segura. La máquina no necesita ser un servidor superpoderoso.

Necesita instalar dos NICs (placas de red) en el gateway VPN, uno para su red poco segura y otra



Figura 3

para la red interna segura. Si usted ha implementado una VPN para usuarios basada en Internet, estará familiarizado con éste proceso. Enchufe el AP inalámbrico- y nada más- directamente en la interface de la red insegura. Cualquiera que se asocie con su AP inalámbrico podrá rastrear solo la interface de su servidor VPN inseguro y cualquier otro cliente asociado con el AP. El servidor VPN se vuelve el gateway para su red interna, decidiendo a quien permite y a quien se rechaza.

Para comunicarse con la interface insegura de su servidor VPN, sus usuarios inalámbricos deben tener una dirección de IP insegura asignada. Si su AP inalámbrico tiene capacidades de servidor DHCP, puede configurar el AP para repartir direcciones IP inseguras a todos los que se asocien (recomendado). Si su AP inalámbrico no tiene capacidades de servidor DHCP, usted puede instalar el servicio DHCP en su servidor VPN y configurarlo para que reparta direcciones IP inseguras solo en la subred de la interface insegura. Por ejemplo, asuma-mos que

Figura 4

Figura 5

la red insegura comprende el rango de direcciones de IP obtenida de 192.168.0.0/24 (con una máscara de 255.255.255.0) y ése AP inalámbrico repartirá una dirección de IP en éste rango a cualquier dispositivo que pida uno. También asuma que la interface de su servidor VPN inseguro tenga una dirección de IP de 192.168.0.65. Para su red interna, asuma que su organización ha usado el rango de dirección IP de 10.18.0.0/16 (con una máscara de 255.255.0.0). Para el segmento de red al que el servidor VPN está conectado, asuma que la dirección de IP está en el rango de 10.18.16.0/24 y que el servidor de VPN tendrá una dirección IP de 10.18.16.10 asignada a la interface segura.

En este punto, si usted colocó el servidor VPN entre su AP inalámbrico y el resto de la red, un usuario inalámbrico puede asociarse con su AP inalámbrico-y eso es todo. El próximo paso es configurar el servidor VPN así puede autorizar apropiadamente a sus usuarios y permitir su acceso dentro de su red interna.

Para comenzar a instalar las capacidades de VPN en el servidor, seleccione Start, Programs, Adminstrative Tools, Routing y Remote Access. Cuando el Microsoft Management Console (MMC) Routing y Remote Access aparezca parpadeando, haga clic (derecho) en el nombre del servidor a la izquierda y seleccione Configure y Enable Routing y Remote Access. Haciendo esto empezará el Routing y el Remote Access Server Setup Wizard.

Microsoft ha simplificado la instalación del servidor VPN (comparado con lo que hay que hacer en el Windows NT 4.0), así que recorriendo las pantallas del wizard se hace sencillo. Veamos cada pantalla, empezando por la pantalla de Common Configurations (configuraciones más comunes), como muestra la figura 3.

Elija instalar un servidor VPN seleccionando Virtual Private Network (VPN) Server. Haga clic ***Next*** para proceder a la pantalla de Remote Client Protocols, como en la figura 4. Ésta pantalla es un poco desconcertante, no tiene demasiado propósito. El wizard provee una lista de protocolos y le pide que asegure que todos los protocolos que necesita para soportar a sus clientes estén instalados en el servidor. Si usted selecciona ***NO, I need to add protocols***, el wizard no le dejará reconfigurar su red de trabajo. Simplemente renuncia. Usted también puede deseleccionar protocolos en ésta pantalla; por ejemplo, para no permitir IPX sobre su VPN. Entonces, si usted tiene los protocolos correctos instalados en su sistema, seleccione ***Yes, all of the available protocols are on this list*** y luego haga clic en ***Next.***

Lo más típico es implementar VPNs a través de Internet que actúa como medio inseguro. Por lo tanto la próxima pantalla wizard, *Internet Connection*, que se muestra en la **figura 5**, pide cuál NIC apunta a su conexión a *Internet*. En este caso considere Internet como sinónimo de **Wireless** y seleccione la interface de red apropiada. En este ejemplo escogimos la interface con la dirección IP 192.168.0.65 que es la dirección que se definió para la conexión a la red wireless insegura. Haga clic en **Next**.

Para dejar a sus usuarios de wireless comunicarse en su red interna, necesita darles una dirección de IP dentro de su espacio interno de la red. A algunos administradores les gusta usar su servidor DHCP primario para ésta tarea (con o sin uso de relay-agents agentes relay de retransmisión)-pero es preferible tener el servidor VPN para repartir direcciones. Al hacer esto ayuda a simplificar fallas.Si usted quiere su gateway VPN asigne direcciones de IP internas a sus usuarios inalámbricos, seleccione **From a Specified range of addresses** en la pantalla IP Adress Assignment, como muestra la **figura** 6, y haga clic en **Next**. Seleccionar ésta opción lo lleva a una pantalla wizard en la cual usted puede definir rangos de direcciones que su servidor VPN puede repartir. Haga clic en **New** en la pantalla para acceder a una caja de diálogo en la cual pude agregar el rango de la dirección de IP apropiada por usar, como en la **figura 7**. Haga clic en **Next** para ir al la última pantalla wizard, que pregunta si se quiere usar un servidor Remote Authentication Dial-In User Service (RADIUS) para autenticar

Asumiendo que quiera utilizar su Active Directory (AD) o la base de datos de un dominio NT para autentificación, responda **No, I don´t want to set this server up to do RADIUS now**, y haga clic en **Next**. Se ha finalizado la instalación de su servidor VPN.

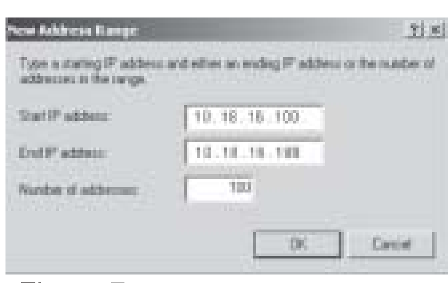


Figura 7



Figura 8

Instalación de un cliente VPN

Para probar la implementación de su nuevo servidor VPN, usted querrá instalar un workstation inalámbrico o laptop y probar cada parte de su conexión: desde el AP inalámbrico al servidor VPN en el lado inseguro de la red y a su red interna.

Si usted bootea su estación de prueba con el NIC inalámbrico, debería poder asociarse con el AP. Puede chequear los drivers provistos por el fabricante de su equipamiento inalámbrico para ver con cuál AP se ha podido asociar. O, si está usando Windows XP, el propio sistema operativo debería decirle a cuál AP inalámbrico está conectado. Verifique que su workstation de

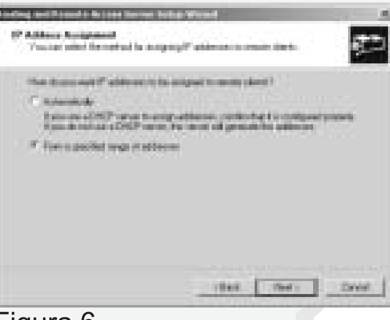


Figura 6

prueba esté recibiendo una dirección TCP/IP insegura del servicio DHCP en su AP (si la configuró para hacerlo) o de su servidor VPN (si instaló DHCP).

Si su workstation de prueba ha obtenido una dirección de IP insegura, usted puede "pinguear" la interface insegura del servidor VPN usando el comando Ping en el command prompt. Haciendo esto se verifica apropiadamente la conectividad de su workstation, del AP inalámbrico y de la interface insegura del servidor VPN. Si obtiene una respuesta exitosa del ping, todo trabaja debidamente hasta ahora. Si no obtiene una respuesta del ping, resuelva el problema antes de continuar.

Ahora es momento de establecer una conexión VPN a su red interna. Desde el desktop del Windows XP o 2000, seleccione **Start, Settings, Network** and **Dial-up Conections**, y haga doble clic en **Add New Connection**.Haciendo esto se lanza el Network Connection Wizard, el cual solicitará la información necesaria acerca de la conexión que quiere realizar. En la pantalla Network Conection Type, **la figura** 8, especifique una conexión VPN seleccionando **Connect to a private network through the Internet.** Haga clic en **Next.**

La próxima pantalla del wizard le pide el nombre DNS o la dirección de IP del servidor VPN al que usted se quiere conectar. Probablemente usted no tenga un DNS disponible para un usuario inalámbrico quien no ha sido propiamente autenticado todavía, así que use la dirección de IP de su interface insegura del servidor PVN: 192.168.0.65, en el ejemplo- y haga clic en **Next**

Las últimas dos pantallas del wizard son simples, preguntando si quiere hacer disponible esta conexión solo para usted o para todos los usuarios. Responda la pregunta apropiadamente según su situación.

Ahora, empieza la diversión. Empiece la conexión DUN y provea un nombre de usuario y passwords en el box de logon (su servidor VPN necesita verificar que su cuenta de usuario ha sido otorgada vía acceso dial-in). Su sistema establece el túnel VPN a su servidor VPN, el cual lo autentica a usted contra la base de datos AD o contra la cuenta local de base de datos. Luego que usted está apropiadamente autenticado, el servidor VPN le asigna a su workstation de prueba una dirección de IP y empieza a encaminar su tráfico a la red interna. Usted puede verificar este ruteo corriendo el Ipconfig en su workstation de prueba y chequeando la dirección de IP que le ha sido asignada. Usted debería ver una dirección segura y una insegura.Ahora tiene una red inalámbrica protegida usando VPN.

Usted se preguntara qué le sucede a los usuarios de laptops que se mueven alrededor de la oficina y van de una AP a otro. Porque cada AP le da un enlace específico de direcciones inseguras, la dirección IP insegura de un usuario que cambia de APs, también cambia. RRAS procura instalar un túnel VPN seguro para la comunicación con el dispositivo del usuario que de repente cambia su dirección IP. Sin embargo el túnel VPN se quebrará. De todas formas si usted selecciona la opción "Redial if line is dropped", cuando usted defina el perfil de la conexión de su cliente, puede estar seguro de que el Windows tratará de reestablecer la conexión cuando haya sido perdida.

IMPLEMENTAR UNA RED DE WIRELESS SIN TOMAR LOS RECAUDOS DE SEGURIDAD NECESARIOS ES COMO TIRAR CABLES DE ETHERNET POR LA VENTANA DE SUS OFICINAS INVITANDO A CUALQUIERA A COMPARTIR SU RED

Entendiendo IPSec

IP básico no tiene seguridad. Pero, para muchas comunicaciones es indispensable. SSL resuelve el problema pero para el caso más restringido de comunicaciones a través de Web browsing.

Si una compañía deseara conectar un Server en sus oficinas en Córdoba con otro en su central en Bs. As. a través de Internet seguramente no permitiría que alguien "snoopeara" la comunicación ni la modificara. Es decir buscaríamos una conexión segura. SSL no seria la solución en este caso.

Otro conjunto de protocolos llamados IP Security o IPSec buscan proveer una respuesta general para seguridad en "networks basados en IP". A diferencia de SSL que opera a nivel de la capa de aplicaciones (SSL es un application-layer protocol) IPSec opera en la network-layer al igual que IP. IPSec es una parte necesaria cuando se usa una conexión VPN (Virtual Private Network) bajo el protocolo de tuneleo L2TP (Layer 2 Tuneling Protocol).

Básicamente, IPSec nos permite tomar dos computadoras y asegurar la conversación entre ellas con diferentes grados de seguridad. Para comprender IPSec necesitamos conocer: IPSec "actions", "filters," and "rules" (acciones, filtros y reglas).

Action types de IPSec

IPSec le permite elegir cuan segura será una comunicación entre computadoras. Ofrece 4 niveles de seguridad ("actions")

-Bloquear transmisiones
-Encriptar transmisiones
-Firmar transmisiones
-Permitir que las transmisiones viajen sin cambios. No se encripta ni se firma

Examinemos estas en más detalle: (Bloquear la transmisión)

Esta opción hace lo que dice: bloquea las transmisiones. Cuando uno le dice a IPSec "bloquee el trafico de maquina X a Y" IPSec en Y simplemente descarta cualquier trafico que viene de X.

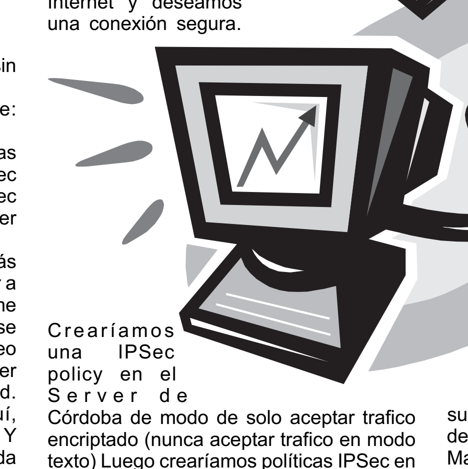
Esta es la opción de seguridad más extrema. Si yo no quiero recibir o permitir a nadie de la subred 200.200.100.0 que me manden mail o visiten mi sitio web o se comuniquen de cualquier forma sólo seteo IPSec en mi sistema descartando cualquier paquete que venga de esa subred.

(Encriptar la transmisión: ESP)Aquí, "quiero" permitir que el trafico pase de X a Y pero estoy preocupado que alguien pueda "pispear" ("eavesdrop") la conexión. Entonces le digo a IPSec que use un protocolo llamado: Encapsulating Security Payload (ESP) para encriptar el tráfico antes de ponerlo en la red, Los Snoopers (husmeadores) solo verán un flujo de bytes de apariencia aleatoria e ilegibles.

Notemos cuán conveniente es que IPSec funciona en la capa "network" de modo que puede encriptar "cualquier cosa". Por ejemplo si te gusta usar telnet pero querés mejorar sobre qué envía la información en modo texto le decís a IPSec que cada vez que X e Y usan telnet para comunicarse que IPSec use ESP para encriptar la comunicación. Nada hay que modificarle a nivel de aplicaciones al servidor ni al cliente Telnet.

Ejemplo de cuando la encriptación seria útil. Quizás uno tenga dentro de una Intranet una maquina que maneja información de importancia como sueldos o tarjetas de crédito. Supongamos que se guarda en SQL1 y es solo editada desde WS1, WS2 o WS3. Supongamos se teme que un "sniffer" de adentro atrape esta información. Uno puede prevenir que se acceda a la base SQL con permisos. Pero no evitara que "escuchen" en la red. Con IPSec esto se puede creando una política en SQL1 que fuerce que cualquier comunicación hacia y desde WS1, WS2 y WS3 este encriptada. Uno debe crear políticas similares en las WS.

Otro ejemplo: supongamos tener un servidor en Córdoba y otras oficinas en distintas ciudades del país. Supongamos que la manera de conectarnos al servidor es a través de Internet y deseamos una conexión segura.



Crearíamos una IPSec policy en el Server de Córdoba de modo de solo aceptar trafico encriptado (nunca aceptar trafico en modo texto) Luego crearíamos políticas IPSec en las workstations de modo de solo comunicarse con el servidor en Córdoba vía ESP.

Transmision firmada: Encabezado autenticado (AH)

En cierto tipo de ataques a redes se engaña a su computadora haciéndoles creer que transmisiones a ella provienen de alguien de confianza. Otro tipo de ataque consiste en interceptar los paquetes transmitidos, modificarlos y hacerlos continuar (lo que se llama "man in the middle attack" (ataque de hombre en el medio). IPSec nos deja proteger este tipo de ataque con un protocolo llamado Encabezado autenticado (AH). AH es un método de firmar digitalmente las comunicaciones. No encriptamos nuestra comunicación y alguien escuchando lo podría hacer. Firma digital agrega un bit de data al final de nuestros paquetes para corroborar que ellos no fueron modificados en el camino.

Transmisión permitida

"Permitido" es en IPSec "sin seguridad". Le dice a IPSec que deje pasar el tráfico sin cambios y sin chequeos de integridad. Es lo que nos da TCP/IP sin IPSec. ¿Para que entonces incluirlo como una acción? De modo de poder crear reglas que restrinjan algunas cosas y no otras: "bloquee todo el trafico que llega "excepto" el trafico en puertos 80 y 443. Permita tráfico solo en esos puertos.

Filtros IPSec

Ahora que sabemos lo que IPSec puede hacer veamos una importante flexibilización de IPSec: sus filtros. En los ejemplos se dijo que queríamos IPSec encriptará entre dos sistemas. En otro dijimos que no solo queríamos encriptar entre 2 maquinas sino que refinara y lo hiciese SOLO CUANDO CORRE TELNET. En la sección de bloqueo se sugirió bloquear al web server todo tráfico desde 200.200.100.0.

Mas específicamente uno puedo usar filtros para restringir IPSec en asegurar la comunicación

Por IP address de la computadora fuente, el IP de la subnet o nombre DNS.

Por IP address de la computadora destino, el IP de la subnet o nombre DNS

Por puerto o tipo de puerto (port type) (TCP, UDP, ICMP, etc))

Todo esto hace IPSec muy flexible:

IPSec Rules = IPSec Actions + IPSec Filters

Bloquear, encriptar, firmar o permitir trafico se dice es una IP action. Y acabamos de ver IPSec filtres. Para usar IPSec uno combina filtros y acciones para producir "reglas" (Rules). Por ejemplo si quiero decirle a IPSec en una dada computadora: "encripte todo el trafico bajo telnet de la computadora en 10.10.11.3". Esa es una "Regla" (Rule). Tiene una parte filtro y una acción:

El filtro dice: "solo active esta regla si hay trafico que es (1) de la dirección IP 10.10.11.3, y (2) cuando use puerto 23 (telnet usa puerto 23)

La parte de la acción dice: "encripte ese trafico".

Windows 2000, XP o .NET server implementan IPSec construyendo políticas. Las políticas están hechas de una o mas reglas. Y, reglas están hechas de filtros (¿Lo debo hacer?) y acciones (¿que debo hacer?).

Firmado y encriptado necesitan una pieza mas: autenticación

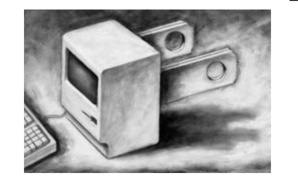
En orden de poder hacer funcionar firmado digital o encriptación se necesita establecer "keys" (llaves) (básicamente password). Así, que cuando uno crea una regla IPSec debe decirle a IPSec como autenticarse.

El IPSec de MS soporta 3 métodos de autenticación: Kerberos, certificados o una llave-concertada (agreed-upon key). Kerberos solo funciona entre computadoras que están en un dominio Active Directory (AD) o en Active Directories que se confían mutuamente. Simplemente tener dos computadoras que tengan clientes Kerberos no será suficiente y aun tener 2 sistemas Windows miembros del mismo "realm Kerberos" (Unix-based Kerberos versión 5 realm) no basta. Quizás MS debería haber llamado a esta opción "Active Directory".

La opción "certificados" le permite usar la PKI (Infraestructura de llaves publicas) para identificar una maquina. La opción "preshared key" (llave pre-acordada) permite usar un string de texto como llave. No muy seguro. Esta opción es muy buena para experimentar. No hay necesidad de establecer certificados o un dominio AD. Solo basta decirle a ambas maquinas usar "preshared key" y escribir cualquier texto como "esto es un secreto" en las maquinas. No seria muy útil en producción pero si para enseñanza.

La implementación de IPSec de MS tiene algo con poco sentido: exige autenticación ya sea que IPSec lo necesite o no. Si uno permite tráfico sin cambiarlo o lo bloquea totalmente en principio no necesita establecer llaves pre-acordadas. Así que en teoría cualquier regla que solo incluya permitir y bloquear no debería requerir ningún método de autenticación.

Pero, MS nos lo pide de todos modos aun cuando no se usa. Así que si estable una regla que solo bloquee y/o permita elija cualquier método de autenticación ya que da lo mismo.
Y cuando usaríamos solo permitir o bloquear'. Cuando uno setea IPSec a realizar una de sus habilidades más interesantes: por ejemplo construir filtros de paquetes muy flexibles.
Como hacemos para activar todo esto. IPSec se maneja por políticas: locales o basadas en el dominio. Uno crea reglas IPSec del Local Security Policy program (secpol.msc) or via Group Policies. Las políticas contendrán una o mas reglas. La mejor estrategia para crear las reglas es definir filtros y acciones primero y luego pegarlas para armar las reglas.
Para empezar, abra Local Security Policy (Start/Programs/Administrative Tools/Local Security Policy) y mire la carpeta labelled "IP Security Policies on Local Machine."
Botón-derecho en ese folder y elija "Manage IP filter lists and filter actions," y cree los filtros y acciones deseadas.
Cierre los diálogos y haga botón-derecho esta vez sobre "Create IP Security Policy" para crear una política.
Una vez que tiene la política como desea haga botón-derecho y asígnela (assign). Ud vera que MS ha pre-creado 3 políticas. Solo una puede estar activa. Así, que si no la asigna no vera su efecto.
Para leer un ejemplo paso a paso del uso de IPSec (para encriptar la comunicación entre 2 maquinas) vea el MS Q article Q301284.



Un libro excelente sobre Windows Server 2003.

El libro está a disposición de aquellos que quieran consultarlo en la biblioteca de COR Technologies. Por favor contactar a biblioteca@cortech.com.ar)

Mastering Windows Server 2003 by Mark Minasi (Editor), Christa Anderson, Michele Beveridge, C. A. Callahan, Lisa Justice

Pocas veces se puede recomendar tan abiertamente un libro. Este es el caso de Mastering Windows Server 2003 por Mark Minasi et al. (Sybex 2004).

Si usted es, o aspira a ser un Administrador o Consultor Windows, no busque más que "Mastering Windows Server 2003" de Sybex (en inglés). Aun ANAYA (quien saco la traducción (hay que decir bastante pobre) al español del libro correspondiente a W2000) aún no lo ha editado. Su cobertura es profunda, comprensible, imparcial y altamente "legible" (algunos incluso dirían "entretenida").Su autor, Mark Minasi es una autoridad en el tema. Construido en la base de años de experiencia trabajando y escribiendo sobre productos Windows, Minasi lo lleva a conocer las tecnologías sobre las que se basa Windows 2003 Server (el sistema operativo de Microsoft que proporciona una solución para compartir archivos e impresoras, conectividad segura en Internet, el desarrollo de aplicaciones de escritorio centralizadas, y la colaboración entre negocios, empleados, y clientes).



Los diferentes temas abordados incluyen:
Configuration de IP, DHCP, DNS, y WINS DNS explicado desde lo básico hasta el diseño avanzado.
El diseño de dominios basados en Active Directory con Server 2003 y 2000 Server. Como tener su propio servidor Web, FTP,y de e-mail con W 2003.
Como controlar cientos e incluso miles de workstations con group policies y templates de seguridad.
Tuning y monitoreo de su red.
Como asegurar su red con split-brain DNS hasta delegación en AD; uso de group policies, logs, IPSec, PKI y mas.
Como utilizar Windows Server 2003 para compartir conexiones a Internet NAT, NAT traversal, Routing y Acceso remoto una completa cobertura de las novedades de W2003.

HPC (High Performance Computing) bajo W2K. Cornell Theory Center

Existen en la actualidad investigaciones científicas, aplicaciones, servicios y desarrollos industriales cuyos proyectos incluyen cálculos de alta complejidad. Esto exige gran capacidad computacional (velocidad de procesamiento, mucha memoria y fiabilidad).

Estas máquinas se las denomina "supercomputers" o HPC.
El mundo del HCP ha verificado un cambio muy grande. Se han reemplazado los mainframes por servidores trabajando en cluster (empresas como *CRAY*, *IBM*, son *sólo ejemplos de quienes proveían esta infraestructura). Esto ha permitido que centros de investigación y empresas puedan tener sus propias "supercomputers" ya que adquieren progresivamente servidores a medida de sus necesidades. El sistema operativo W2K ha permitido a Microsoft participar en dar soluciones de HPC.*
La primera implementación en supercomputación sobre Microsoft Windows 2000 la realizó el Cornell Theory Center. Se construyó el *AC3 Velocity Cluster. Éste es un cluster basado en el sistema operativo* W2K, *formado por 256 procesadores de Intel distribuidos en 4 servidores Power Edge de Dell. La conexión se realiza mediante adaptadores de host cLAN y switches de cluster. Es de destacar que la Universidad de Cornell firmó un acuerdo con Microsoft, Intel y Dell de modo de desarrollar conjuntamente soluciones y servicios comerciales de HPC destinados a la industria, gobierno y ámbitos de investigación.*
¿Quiénes necesitan tanto poder de cálculo? Estos abarcan complejos trabajos de física, investigación espacial, desarrollo de nuevos productos farmacéuticos, estudios de aerodinámica en la industria aeronáutica, diseño de automóviles, simulaciones de terremotos, predicción meteorológica, astronomía, representaciones 3D o estudios de cambios climáticos. Tales proyectos no se podrían realizar sin la ayuda de tales cerebros informáticos.

Para más información:

www.research.microsoft.com
www.tc.cornell.edu
Www.microsoft.com/windows2000/hpc/

MCSA Y MCSE A FONDO.

Microsoft CERTIFIED Systems Engineer

Microsoft CERTIFIED Systems Administrator

Certificaciones Microsoft: MCSA y MCSE

Las certificaciones de Microsoft acreditan los conocimientos y la competencia de los profesionales en el manejo de productos Microsoft. Si representa a un negocio que busca líderes en tecnología o es un profesional de la tecnología de la información que quieren convertirse en ese tipo de líder, el programa de Microsoft Certified Professional (MCP) es lo que está buscando.

Como un profesional de informática (IT), tiene la opción de lograr dos credenciales diferentes para destacar su conocimiento y experiencia en Microsoft Windows® 2000/2003 o Microsoft Windows® XPMicrosoft Certified Systems Administrator (MCSA) y Microsoft Certified Systems Engineer (MCSE). ¿Qué certificación es la adecuada para usted y su rol de trabajo?

Elija la credencial MCSA si usted:

Administra, brinda soporte y soluciona problemas de las continuas necesidades de los entornos operativos de servidor de Microsoft Windows®.

Tiene 6 a 12 meses de experiencia administrando y brindando soporte a operaciones de servidor de escritorio y redes en una infraestructura de red existente.

Los ejemplos de puestos de trabajo incluyen: administrador de sistemas, administrador de redes, administrador de sistemas de información, analista de operaciones de redes, técnico en redes o especialista en soporte técnico.

Elija la credencial MCSE si usted:

Planifica, diseña e implementa soluciones y arquitecturas de servidor de Microsoft Windows.

Tiene al menos un año de experiencia analizando requerimientos de negocios y técnicos como planificando, diseñando e implementando soluciones con productos y tecnologías de Microsoft.

Los ejemplos de puestos de trabajo incluyen: ingeniero de sistemas, ingeniero de redes, analista de sistemas, analista de redes o consultor técnico.

MCSA (Microsoft Certified System Administrator)

La certificación Microsoft Certified Systems Administrator (MCSA) para Microsoft Windows 2000 y Windows 2003 está pensada para profesionales encargados de implementar, administrar y solucionar problemas de entornos de red y de sistemas existentes basados en las plataformas Microsoft Windows® 2000 y Windows® 2003. Entre las responsabilidades de la implementación figuran la instalación y configuración de los componentes de los sistemas. Entre las de administración, la administración y el soporte técnico de los sistemas.

La credencial MCSA para Microsoft Windows 2000 y Windows 2003 satisface sus necesidades

La demanda de puestos de trabajo para administrar redes ha crecido de manera importante en los utlimos años. Ante esta situación, tanto los candidatos como el sector han manifestado la necesidad de crear una certificación para este perfil de trabajo.

La certificación MCSA para Windows 2000 y Windows 2003 supone una ventaja competitiva para los profesionales de IT que trabajan en el entorno empresarial actual, en constante desarrollo, puesto que valida la experiencia específica que requiere la función del administrador de redes y sistemas. La certificación proporciona a las empresas una manera de identificar a los profesionales cualificados y con el conjunto de conocimientos adecuado para realizar el trabajo correctamente.

La certificación MCSA para Windows 2000 y Windows 2003 es adecuada para

Administradores de redes

Ingenieros de redes

Administradores de sistemas

Profesionales de tecnologías de la información

Administradores de sistemas de información

Técnicos de redes

Especialistas de soporte técnico

Entorno informático habitual de MCSA

La credencial MCSA para Windows 2000 y Windows 2003 está destinada a profesionales de TI que trabajan en entornos de equipos normalmente complejos de la mediana y gran empresa. Los candidatos a la certificación MCSA para Windows 2000 y Windows 2003 deben tener entre seis y doce meses de experiencia en la administración de sistemas operativos cliente y de red en entornos con las siguientes características:

Admiten de 200 a 26.000 usuarios o más.

Admiten de dos a 100 ubicaciones físicas.

Entre los servicios y recursos típicos de red figuran la mensajería, bases de datos, archivos e impresión, servidor proxy o servidor de seguridad, Internet e intranet, acceso remoto y administración de equipos cliente.

La conectividad exige la conexión de sucursales y usuarios individuales de ubicaciones remotas a la red corporativa, y la conexión de redes corporativas a Internet.

Empleo de múltiples plataformas con el objetivo de permitir interoperabilidad y compatibilidad con Microsoft Windows Networks.

MCSE (Microsoft Certified System Engineer)

La acreditación Microsoft Certified Systems Engineer (MCSE) es la certificación superior para los profesionales que analizan los requisitos

Beneficios derivados de la obtención de la certificación MCSA: Security

Todas las certificaciones Microsoft (MCP, MCSA, MCSE, MCDBA, MCAD, MCSD, MCDST) poseen beneficios importantes. A modo de ejemplo hemos trascripto los pertenecientes a la Carrera MCSA Security.

El reconocimiento del sector de su competencia y conocimiento de los productos y tecnologías de Microsoft.
El acceso a información técnica y sobre productos directamente desde Microsoft a través de un área de seguridad del sitio Web MCP .
El acceso a descuentos exclusivos en productos y servicios de determinadas empresas. Aquellos profesionales que ya sean MCPs (Microsoft Certified Professionals) podrán disfrutar de estos beneficios al visitar las áreas seguras del sitio MCP .
El logotipo, trascripción, tarjeta y pin de la certificación MCSA: Seguridad en Windows 2000 para poder identificarse como un MCP ante sus compañeros de trabajo y clientes. Se pueden descargar archivos electrónicos de logos y transcripciones desde el sitio seguro de MCP si se dispone de certificación.
Invitaciones a conferencias, sesiones de formación técnica y eventos especiales.
Acceso gratuito a *Microsoft Certified Professional Magazine Online*, una revista del sector dedicada al desarrollo profesional. Entre los contenidos sobre mejoras en seguridad de la revista *online* que aparece en el sitio Web de *Microsoft Certified Professional Magazine Online* se incluye el último número (disponible solo para MCPs), otros artículos y contenidos *online* , una base de datos sólo para MCP y chats frecuentes con expertos técnicos de Microsoft o de otras compañías. Además se ofrecen otros beneficios *online* para los particulares que dispongan de la certificación MCSE+Internet, MCSE, MCSD y MCDBA. Visite el sitio privado de MCP para acceder a la revista *Microsoft Certified Professional Magazine Online*. (Todos los MCPs pueden optar a consultar los contenidos sobre seguridad de esta revista. Algunos también pueden optar a recibir la versión impresa de la revista de manera gratuita; la decisión de quién puede optar o no la toma la revista.)
Un trato especial en la suscripción a *Windows & .NET Magazine*, una de las principales fuentes de información independiente y formación para profesionales TI que trabajan en una plataforma de Windows. Visite el sitio seguro de MCP si quiere información más detallada.
Algunos beneficios por la obtención y validez del titulo a nivel mundial
Reconocimiento Internacional de su profesionalidad y conocimientos avanzados en Productos Microsoft así como de sus tecnologías.
Mejores salarios al ser más competitivo y reconocido.
Clientes confiados y seguros de que sus servicios son únicos e inmejorables

Otras credenciales de Microsoft

Microsoft ofrece otras credenciales además de MCSA y MCSE.

Microsoft Certified Professional (MCP) alguien que pase un examen de certificación, por ejemplo, es reconocido por Microsoft como un experto en ese producto.
MCDT (Microsoft Certified Desktop Support Technician) es un excelente entry level (comienzo de carrera). Al obtener esta certificación demuestra que dispone de las habilidades necesarias para solucionar los problemas que surjan en entornos de escritorio en los que se esté ejecutando un sistema operativo de Microsoft Windows.

MCDBA(Microsoft Certified Data Base Administrador) para aquellos con interés en manejo de bases de datos.

MCSD (Microsoft Certified Solution Developer) es la certificación idónea para profesionales que diseñan y desarrollan las últimas soluciones empresariales con herramientas de desarrollo, tecnologías y plataformas de Microsoft y con arquitectura Microsoft Windows.
MCAD (Microsoft Certified Application Developer) para quienes desarrollen aplicaciones y web services con .NET
Microsoft Office Specialist reconoce los conocimientos y habilidades con las aplicaciones de escritorio de Microsoft.
MCT (Microsoft Certified Trainer): la certificación para aquellos que quieran dedicarse a la capacitacion .

empresariales y diseñan e implementan la infraestructura de las soluciones empresariales basadas en la plataforma Microsoft Windows® 2000 y Windows 2003 y en el software de servidor de Microsoft. Las responsabilidades de la implementación incluyen la instalación, la configuración y la resolución de problemas de los sistemas de red. Para obtener más información acerca de las funciones de un MCSE, lea el documento MCSE Job Task Analysis (http://www.microsoft.com/latam/entrenamiento/downloads/MCSE_Task_Analysis.doc).

La certificación MCSE es apropiada para los siguientes profesionales:

- Ingenieros de sistemas
- Ingenieros de soporte técnico
- Analistas de sistemas
- Analistas de redes
- Consultores técnicos

La acreditación MCSE es una de las certificaciones técnicas de mayor prestigio del sector. Al obtener la acreditación MCSE superior, los profesionales demuestran tener los conocimientos necesarios para liderar con éxito el diseño, la implementación y la administración del sistema operativo Microsoft Windows más avanzado y de los productos de servidor de Microsoft.

El entorno informático típico de un MCSE

La credencial MCSE de Windows 2000 y Windows 2003 está diseñado para los profesionales de las tecnologías de la información que trabajan en los entornos informáticos complejos característicos de las organizaciones de tamaño mediano y grande.

Un candidato a MCSE debe contar al menos con un año de experiencia en la implementación y administración de un sistema operativo de red en un entorno de las siguientes características:

- De 200 a 26.000 usuarios
- De 5 a 150 sedes físicas
- Servicios y aplicaciones de red habituales: archivos, impresión, bases de datos, mensajerías, servidor proxy o servidor de seguridad, servidor de acceso telefónico, administración de escritorios y hospedaje Web
- Conectividad, incluida la conexión de oficinas y usuarios remotos a la red corporativa y la conexión de redes corporativas a Internet
- Diseño de Infraestructura de redes y de Directorio Activo (Active Directory)
- Diseño de Seguridad de la red Local y exposición de la misma en la red Publica de la Internet.
- Empleo de múltiples plataformas con el objetivo de permitir interoperabilidad y compatibilidad con Microsoft Windows Networks.

¿Dónde se pueden hacer los exámenes para certificarme como MCSA y/o MCSE ?

Podes hacer los exámenes en cualquier centro CTEC (Certified Training Education Center) de tu localidad que provea exámenes ya sean de VUE (Virtual Universities Enterprise) o Sylvain Prometic. Los exámenes se separan con anticipación y tienen un costo de 125.00 USD en U.S.A. cada uno; y 80.00 USD en Argentina (tarifas adicionales o descuentos pueden aplicarse en otras regiones).

Los exámenes son basados en "ambientes" o enviroments. En estos se hacen preguntas por separado con cada ambiente, y las preguntas pueden ser de múltiple opción, de arrastrar y soltar, llenar tablas, etc.

Ahora también Microsoft introduce nuevas tecnologías de Seguridad en estos examenes, incluyendo tecnologia Adaptiva y elementos de Simulación (http://www.microsoft.com/traincert/mcpexams/faq/security.asp) . Estos nuevos tipos preguntas en los exámenes para el MCSA y MCSE representan una visión mas realista de los productos que se están examinando por lo que la experiencia al tomar el Test reflejan mas consistentemente las diferentes tipos de tareas que uno se encontraría en la labor de una Administrador de Redes en la vida real.

Aquellos que hayan realizado la Carrera MCSA y MCSE en Windows 2000 podrán hacer la correspondiente actualización (un examen para MCSA, 70-292 y dos Exámenes para MCSE 70-292 y 70-296) y recibir el correspondiente status de MCSA o MCSE bajo Windows 2003

¿Cómo me preparo para obtener mi MCSA?

Existen diferentes metodologías para prepararte para ser un MCSA o un MCSE. Algo que es muy importante es que hay que dedicarse. Vas a necesitar poner todo de tu parte, ya que estamos hablando de un Status muy reconocido como estudios superiores de una Universidad muy reconocida, por lo que debes poner todo tu esfuerzo para lograr esta meta.

Los estudios para lograr el MCSA y MCSE pueden requerir sesiones de estudio y jornadas largas de entrenamiento que incluyen laboratorios, practicas y sesiones reales para simular ambientes empresariales reales, los cuales te ayudaran a entender mejor los objetivos y te harán tomar decisiones y acciones indispensables como un verdadero profesional de las Tecnologías de la Información. Entre los recursos que puedes tener en cuenta para tu preparación se encuentran:

- Cursos MOC (Microsoft Official Curriculum) en tu CTEC (Certified Training Education Center).
- Practicas y Laboratorios (Hands On practices). (Ej: Transcenders en http://www.transcender.com/)
- Experiencia real en ambientes Microsoft.
- Leer Guias de Estudio Online.
- Estudiar el Material de Microsoft Press (http://www.microsoft.com/mspress/)
- Compartir Experiencias en Forums de Discusion, etc

¿Cuáles son los Exámenes que debo tomar para recibirme de MCSA o MCSE ?

Existen muchísimas combinaciones de Exámenes para recibirse de MCSA y MCSE. Cada una con diferentes especializaciones y electivos para tomar. Te recomendamos que bajes los PDFs correspondientes a las Carreras MCSA Windows 2000 y Windows 2003; y MCSE Windows 2000 y Windows 2003 de los siguientes links.

MCSA

http://www.cortech.com.ar/gen/mcsawin2003.pdf
http://www.cortech.com.ar/gen/MCSASec2000-2003.pdf
http://www.cortech.com.ar/gen/MCSAMes2000-2003.pdf

MCSE

http://www.cortech.com.ar/gen/mcsewin2003.pdf
http://www.cortech.com.ar/gen/MCSESec2000-2003.pdf
http://www.cortech.com.ar/gen/MCSEMes2000-2003.pdf

Algunos links interesantes para obtener las credenciales MCSA y MCSE

http://www.transcender.com/products/demos.asp
http://www.selftestsoftware.com
http://www.cert21.com
http://www.mcpmag.com

Especializaciones en las certificaciones MCSA y MCSE : Security y Messaging

Ambas certificaciones de Microsoft en infraestructura de redes (networking) son interesantes de lograr. Pero, Microsoft ha agregado recientemente dos ESPECIALIZACIONES a cada certificación. Las especializaciones permiten a los individuos focalizarse en tópicos específicos. Estas son Security y Messaging. La primera certifica el conocimiento profundo en el área de seguridad. Messaging demostrará experiencia con Microsoft Exchange. Ambas requerirán a quien posea el titulo MCSA o MCSE tener exámenes adicionales propios de la temática elegida.

Microsoft CERTIFIED Systems Administrator SECURITY | Microsoft CERTIFIED Systems Administrator MESSAGING | Microsoft CERTIFIED Systems Engineer SECURITY | Microsoft CERTIFIED Systems Engineer MESSAGING



¿Por qué los javeros son las cabezas más buscadas por las empresas?

En users**.code #02,** un informe completo con todo lo que hay que saber sobre la actualidad de Java y mucho más...

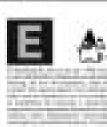
News (!)







MUNDO JAVA





[white paper]

Patrones de arquitectura de aplicaciones



Menús dinámicos en ASP.NET





Las tabla Menu



Java Studio Creator



HARDkey.NET





Generalidades de la ISO / IEC 17799

Código de práctica para la Administración de Seguridad de la Información

ISO /IEC 17799 es el modelo internacional que propone los estándares sobre cómo las empresas deberían conducir el manejo de sus requerimientos de información de seguridad. Está basado en el estándar Británico BS 7799-1:1999.

Un cierto número de diferentes "estándares sobre seguridad" fueron publicados en los diez últimos años por diferentes entidades. Estos estándares incluyen varias publicaciones de entidades como el Instituto Nacional de Ciencia y Tecnología de EE.UU. (NIST) (The US Body National Institute for Science and Technologies) ver www.nist.gov, el informe técnico ISO/IEC de Gerenciamiento de la Seguridad en IT (General Managment of IT Security - GMITS), la Fundación Internacional de Seguridad de Información (the Internacional Information Security Foundation - I^{2}SF), los Principios Generalmente Aceptados de Seguridad de Sistemas (Generally Accepted System Security Principles - GASSP), los Principios de Seguridad OECP (the OECP security principles). También los estándares se definen en los siguientes sitios de Internet:

http://www.e-security-e-comerce-security.com

http://www.information-security-polices-and-standards.com

http://www.information-security-policies.com

Http://www.iso17799software.com

(La) ISO/IEC 17799 está constantemente ganando mercado como estándar internacionalmente aceptado e implementado, habiendo sido exigido para el uso de todos los departamentos gubernamentales de Gran Bretaña y también adoptado en Australia, Brasil, Japón, Países Bajos y Suecia.El estándar identifica un número de "factores de éxitos decisivos" (critical success factors) que una organización debe lograr si desea tener éxito implementando seguridad de la información.

Esto incluye: tener políticas que reflejen los objetivos de negocios, usar una metodología que sea consistente con la cultura institucional, el compromiso de la gerencia, una buena comprensión de los requerimientos, una efectiva política de promulgación, entrenamiento y educación adecuada, y una realimentación ("feedback") que asegure una constante mejora.Más de 100 controles potenciales están identificados, divididos en doce temáticas generales. Estos controles han sido considerados apropiados para representar las necesidades en materia de seguridad de la información de la mayoría de las organizaciones, ya sea que la información se mantenga en papel o almacenada en sistemas de computación.

Pequeñas y medianas empresas (PyMes) pueden no necesitar considerar todos los controles, o pueden confiarse en la capacidad de productos comerciales para proporcionar y respaldar los controles que necesitan. Los departamentos gubernamentales pueden necesitar tener en cuenta además el conjunto de políticas reguladas por la seguridad nacional que pueden agregar requerimientos no contemplados por el ISO/IEC 17799. Los bancos y organizaciones similares pueden también necesitar tener políticas que excedan los puntos listados en el estándar.Hay un estándar separado, BS 7799 parte 2:1999, que detalla los requerimientos que debe cumplir una organización que desea certificar sus procesos de administración: The Information Security Management System ISMS (el Sistema de Administración de Seguridad de la Información).

El "modus operandi" general para este tipo de certificaciones va a resultarle familiar a los que ya están certificados bajo normas ISO 9000/14000. La diferencia más sobresaliente es la necesidad de haber llevado a cabo el proceso de análisis de riesgos, haber hecho justificaciones para los controles que fueron seleccionados, que hay un proceso de continuo mejoramiento y que los controles de administración operan correctamente y son adecuados para su propósito. Si una organización ya tiene sus procesos de administración de seguridad de la información evaluados bajo ISO 9000/14000, la extensión de los requisitos para BS 7799-2 no debería ser demasiado grande u onerosa.

FAQ sobre la ISO 17799

P: ¿Qué es la ISO 17799?
R: La ISO 17799 es una guía de buenas prácticas de seguridad informática que presenta una extensa serie de controles de seguridad. Es la única norma que no sólo cubre la problemática de la IT sino que hace una aproximación holística a la seguridad de la información abarcando todas las funcionalidades de una organización en cuanto a que puedan ser afectadas por la seguridad informática.

P: ¿Es certificable la ISO 17799?
R: Definitivamente no. La ISO 17799 sólo hace recomendaciones sobre el uso de controles de seguridad. No establece requisitos cuyo cumplimiento pudiere certificarse.

P: ¿Por qué hay confusión en el tema de la certificación?
R: En gran parte se debe a los errores de traducción de la norma. El original en inglés de la ISO 17799 usa la expresión verbal "should", un término presente en algunas normas ISO y también del IETF, que por convención expresa una forma condicional a modo de recomendación y no de imposición.

P: Si la ISO 17799 no es certificable, ¿para qué sirve?
R: La ISO 17799 es prácticamente igual a la Primera Parte de la norma BS 7799, o sea la BS 7799-1. Esta norma británica tiene una Segunda Parte, BS 7799-2, que usa la expresión verbal "shall", otro término habitual en ciertas normas para expresar mandato u obligación. Los requisitos que se especifican de esta manera se refieren a un Plan de Seguridad constituido por un Sistema de Gestión de Seguridad Informática (SGSI), en el que se aplican los controles de seguridad de la BS 7799-1 (y por lo tanto de la ISO 17799). Los requisitos que se establecen en el SGSI de la BS 7799-2 se pueden auditar y certificar. No hay versión ISO de la BS 7799-2.

P: ¿Además de su capacidad de ser certificable, qué otras características tiene la BS 7799-2?
R: El cumplimiento de la nueva versión de esta norma, BS 7799-2:2002, constituye el aseguramiento idóneo para las empresas que comparten extranets (como en B2B), así como para los bancos conforme los requisitos del Nuevo Acuerdo de Capitales Basilea II. También proporciona una interesante armonización con otras normas (como la ISO 9001 de Calidad) con el consiguiente beneficio de reducción de esfuerzos y costos.

P: Entonces, ¿en cuanto a gestión de la seguridad informática es suficiente con la BS 7799-2?
R: No exactamente, porque en primer lugar el detalle de los controles de seguridad sólo está en la BS 7799-1 (y por lo tanto en la ISO 17799). La BS 7799-2 muestra cómo aplicar dichos controles y construir el plan de seguridad correspondiente.

Tópicos de los Códigos de Práctica de la ISO 17799

ISO 17799 es un estándar sobre seguridad de la información publicada por la International Organization for Standardization en 2000. Está basada en un estándar anterior : el British Standard 7799, titulado *Information technology - Code of practice for information security management.*Mientras que el propósito de la ISO 17799 está restringido a solamente un código de práctica, el BS 7799 tiene 2 partes. La segunda es llamada *Information Security Management - Part 2: Specification for information security management systems.*Ambos de estos estándares son reconocidos universalmente. Para la segunda parte del BS 7999 (Information Security Management Systems) (ISMSs) existe un sistema de certificación muy reconocido. ISO 17799 y la primera parte de BS 7799 nos proveen de "recomendaciones para el management (administración) de la seguridad de la información para ser usado por aquellos… responsables de… implementar… seguridad en sus organizaciones". La segunda parte de la BS 7799 nos da los requisitos para la ISMSs.

El código de práctica cubre los siguientes tópicos:

Políticas de seguridad

Seguridad en la organización

Clasificación y control de nuestros activos (assets)

Seguridad del personal

Seguridad física y del entorno

administración de comunicaciones y operación

Control de acceso

Desarrollo y mantenimiento de sistemas

Administración de la continuidad del negocio

Compílanse (conformidad)

Referencias

BS ISO/IEC 17799:2000

BS 7799-2:1999

Excelentes links

Official source of ISO 17799 from the British Standards Institute (BSI) (*http://www.standardsdirect.org/iso17799.htm*)

The ISO 17799 Forum (*http://www.17799.com*)

The ISO 17799 Newsletter (*http://www.iso17799-web.com*)

The ISO 17799 security portal (*http://www.iso17799software.com*)